NCP Secure Entry Client

Administration Guide

© NCP engineering GmbH

Version 13

Next Generation Network
Access Technology

secure   efficient   ease of use   mobile

www.ncp-e.com

Contact

For more information or questions about NCP products and services:

Germany
NCP engineering GmbH
Dombühlerstraße 2
D-90449 Nürnberg
Tel.: +49 (911) 9968 0
Homepage: http://www.ncp-e.com
Mail: info@ncp-e.com

E-Mail Support:
support@ncp-e.com (german)
helpdesk@ncp-e.com (english)

Support Hotline:
0900 / 1 99 68 00
(only available from Germany, 80 Cent / per minute)
Our support times are from monday to friday from 08:00 am to 17:00 pm.

Contact USA, North American HQ
NCP engineering, Inc.
19321 US Highway 19 N, Suite 401
Clearwater, FL 33764
Phone: +1 (650) 316-6273

For a support request we need the following information:
- exact product name
- serial number
- version number
- precise description of the problem
- any error message(s)

NCP Secure Entry Client

While considerable care has been taken in the preparation and publication of this manual, errors in content, typo-graphical or otherwise, may occur. If you have any comments or recommendations concerning the accuracy, then please contact NCP. NCP makes no representations or warranties with respect to the contents or use of this manual, and explicitly disclaims all expressed or implied warranties of merchantability or suitability of use for any particular purpose.

Furthermore, NCP reserves the right to revise this publication and to make amendments to the contents, at any time, without obligation to notify any person or entity of such revisions or changes. This manual is the sole property of NCP and may not be copied for resale, commercial distribution or translated to another language without the express written permission of NCP engineering GmbH. All trademarks or registered trademarks appearing in this manual belong to their respective owners.

Table of contents

Product Description
Universal IPsec Client

The IPsec Client can be used in any VPN environment and uses standardized IPsec protocols to communicate with the gateways provided by a wide variety of vendors. The client software emulates an Ethernet LAN adapter, and includes a number of additional features that introduce the user into a holistic remote access VPN solution.

The graphical user interface of the client provides transparency during the connection establishment process and while the data connection is in use. Among other things it provides information on actual data throughput.

IPsec Client Features

• Support of all major Microsoft Windows operating systems (Windows 10). Also available as OS X or Android Client.

• Independence from transmission medium (media type neutral)

• Support of all major operating systems and a wide variety of end devices

• Security and manageability because it is independent from Microsoft RAS

• Communication with IPsec gateways, including those from third-party manufacturers (compatibility)

• Installation on standalone and LAN-based PCs (even behind IP routers with IP-NAT)

• Integrated Personal Firewall [11]

• Domain dial-up (Credential Provider) [207]

• Extended Authentication [185] (XAUTH) for authentication via user ID and password

• Internet Key Exchange Config Mode (IKE CFG) [188] for dynamic allocation of IP addresses, DNS server, Windows Name Server and domain name

• Dead Peer Detection (DPD) [180]; Configuration in case of tunnel failover user configurable time intervalls for DPD for flexible controll of re-building of VPN tunnels.

• Supports the Extensible Authentication Protocols (EAP) [114] with the functions of Transport Layer Security (TLS) and MD5 (user ID / password) for secure authentication of the user to access points or switches

• Network Address Translation - Transversal (NAT-T) for communication between client and gateway via network components which process NAT

• Intelligent Line Management for minimizing transmission costs and increasing transparency (Charge Manager)

FIPS Certification

The IPsec Client incorporates cryptographic algorithms conformant to the FIPS standard 140-2. The embedded cryptographic algorithms has been validated with certificate #1747.

FIPS conformance will always be maintained when the following algorithms are used for establishment and encryption of the IPsec connection:
• Diffie Hellman Group: Group 2 to 14 (DH length of 1024 bits up to 2048 bits)
• Hash Algorithms: SHA1, SHA 256, SHA 384, or SHA 512 Bit
• Encryption Algorithms: AES with 128, 192 or 256 Bit or Triple DES

The respective modules can be configured in the IPsec General Settings 162.

Personal Firewall

The client provides all the personal firewall functionalities to fully secure the workstation against attacks from the Internet, wireless LAN, or the local network. This shield consists of IP-NAT (Network Address Translation) and various IP-protocol filters. NAT is a security standard that prevents exposing the internal private IP address to the Internet by translating it to a legal or public IP address, thus enabling the host (e.g. user PC) to communicate safely across the Internet. Incoming packets are checked for precisely defined properties (address and protocol) in accordance to a sophisticated filter, which rejects those that match the defined parameters. Source ports are also screened to prevent any masquerading. In other words: The Internet port of the respective computer is thoroughly protected, and the building of any unwanted links is prevented.

PKI Support

Strong authentication through digital certificates as soft certificates (PKCS#12) or on smartcards (PKCS#11, CT-API, PC/SC) increases the security for the PC as well as the corporate network. The client becomes part of a Public Key Infrastructure (PKI). Following some PKI elements are described.

Public-Key Infrastructure

PKI consists of a combination of standards, products, guidelines, and procedures. As such it provides the basic security platform for eCommerce business transactions, so those users (un)known to each other can safely communicate. PKI is a globally recognized and applied technology for security.

PKI includes the use of digital certificates that act as personal "electronic ID's" and are issued by a Certificate Authority (CA) or Trust Center. Security experts and the IETF (Internet Engineering Task Force) have concluded that an effective protection against man-in-the-middle attacks can only be achieved by using smartcards with certificates.

Thus, a trust relationship, as we know it in the traditional world of paper-based business, can also be established in the world of global electronic information exchange. A digital signature in combination with data encryption is the electronic equivalent to a written signature and proves the validity and origin of messages in a similarly secure manner.

Smartcard

Smartcards are the ideal enhancement for high security Remote Access solutions. They provide two-fold security for Log-in purposes, which includes the PIN (Personal Identification Number) as well as the actual possession of the smartcard itself. The user identifies himself as the smartcard's rightful owner by entering its assigned PIN (Strong Security). The PIN substitutes the entering of password and user ID (basis for Single-Sign-On). The user identifies himself only to the smartcard. The validation against the network is negotiated between thesmartcard and the corresponding security (authentication) system. All security related processes are executed inside the card, thus not in the PC. Smartcards also provide the technological basis for multi-functional applications, e.g. Company Card, etc.. Biometric processes can also be integrated.

Supported interfaces and formats

The secure client can be used in public key infrastructures as of X.509. V.3 standard and supports the following interfaces/formats:

• Smartcards, USB-Tokens: PKCS#11, TCOS 1.2 and 2.0, CSP

• Soft Certificates: PKCS#12-file

• PC/SC conform smartcard reader: The client software supports all smartcard readers which conform with PC/SC. The smartcard readers are included in a list of the client once the reader is connected and the corresponding driver software has been installed.

• Automatic recognition of connected PC/SC readers: If the use of a PC/SC smartcard reader is configured on the client for the PKI environment, the client recognizes and automatically uses the connected one.

This feature can only be used in connection with smartcards which can be addressed directly without interface software such as NetKey chip cards (Telesec).

• PKCS#11 module: Drivers in form of a PKCS#11 library (DLL) are supplied with the software for smartcards or tokens. This driver software has to be installed initially. Then the relevant PKSC#11 module can be selected via an assistant.

CA Certificates

The administrator of the company network determines which certificate issuers can be trusted. This happens by applying the CA certificate of his choice into the installation directory under [CACERTS]. The application can happen automatically during software distribution if the issuer certificates are located in the directory [DISK1] during software installation from a data carrier.

Retrospectively, issuer certificates can be distributedas long as the user has the relevant write permissions in the relevant directory.

Currently the formats *.pem and *.crt are supported for issuer certificates. They can be viewed in the monitor under the main menu item "Connection / Certificates / Display CA certificates".

If the secure client receives the certificate of a remote station, then the client will determine the issuer by searching the issuer certificate initially on smartcard or USB token or in the PKCS#12 file and finally in the installation directory under [CACERTS]. If the issuer certificate cannot be found then the

connection will not be successful. If no issuer certificates are available, then no connection is allowed.

Use of a Revocation List (CRL)

The secure client can have access to the corresponding CRL (certificate revocation list) for each issuer certificate. It is applied to the installation directory under [CRLS]. If a CRL is available, then the secure client checks incoming certificates against the CRL. The client downloads the corresponding CRL automatically if the incoming server user certificate includes the certificate extension CDP.

If black lists are used, then usually there is no notification if the client has no saved black list for incoming certificates. If a notification is required in such cases then the file NCPPKI.CONF needs to be edited. It is saved in the installation directory. The default entry in the section [General] is:

Enablecrlinfo = 0

This means that no notifications are displayed if, on the client at the remote station, no black list was found for the certificate. If a notification has to be displayed, then this setting has to be changed to:

Enablecrlinfo = 1

Installing the Software

A setup program performs the installation of the Client Software quickly and smoothly. The installation procedures for all versions of NCP Client Software are the same.

Prior to executing installation, make sure that the following prerequisites are fulfilled.

Release Notes

Prior to executing installation, notice the Release Notes.

Remote Gateway

The remote gateway has to support one of the following communication media: PSTN, Mobile Network, LAN over IP or Wi-Fi.

License Key

Software Updates and License Keys

From the current software version, every new major release will require a specific license key for the same version.

A license update is required with the software update when updating the client software via SEM. If the software is updated without performing a license update, the client will receive a license for the remainder of the 30-day trial period.

New Installation and License Keys

For a new installation, the client software is installed under the Program Files directory (previously Program Files (x86)) and licensed as a trial version [17] (for a maximum of 30 days) until a valid license is entered.

To start the installation of the NCP Secure Entry Client, use the installation file. The installation starts with selecting the language of the installation wizard.
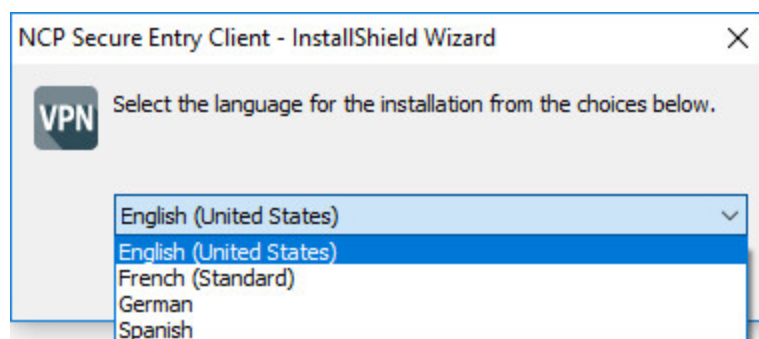
The installation wizard (InstallShield Wizard) is being prepared. The "Welcome window" appears. Click "Next" to start the installation.
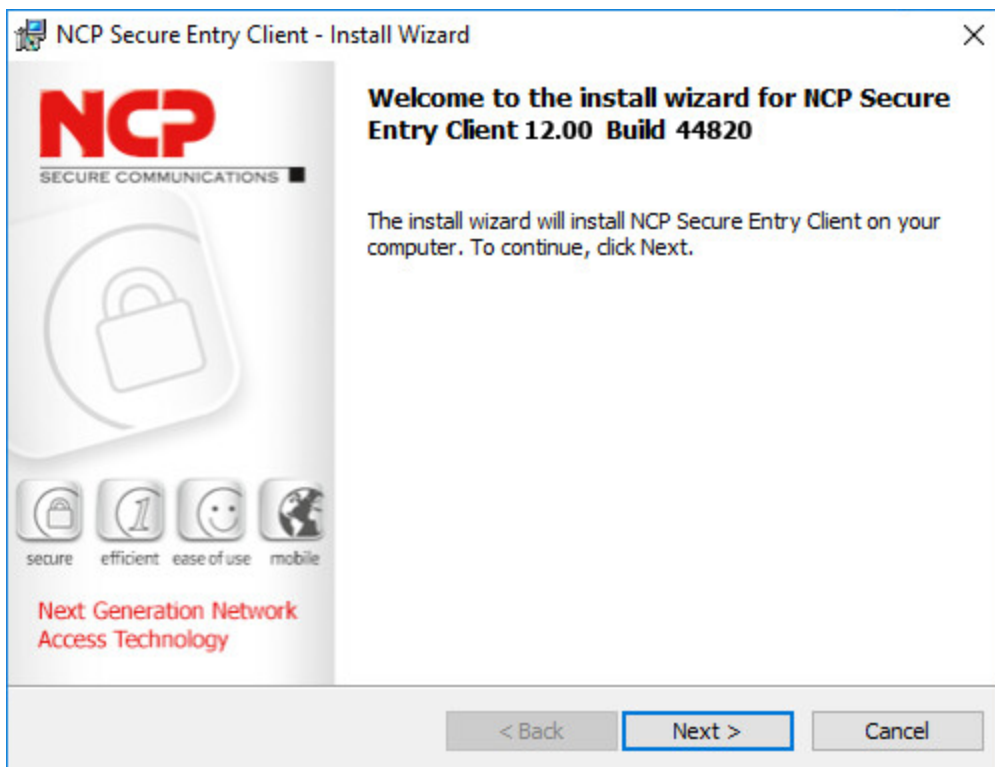
Click "Next" and read the license agreement carefully. To continue the installation, accept the license terms. Reject the license terms or click "Cancel" to cancel the installation.
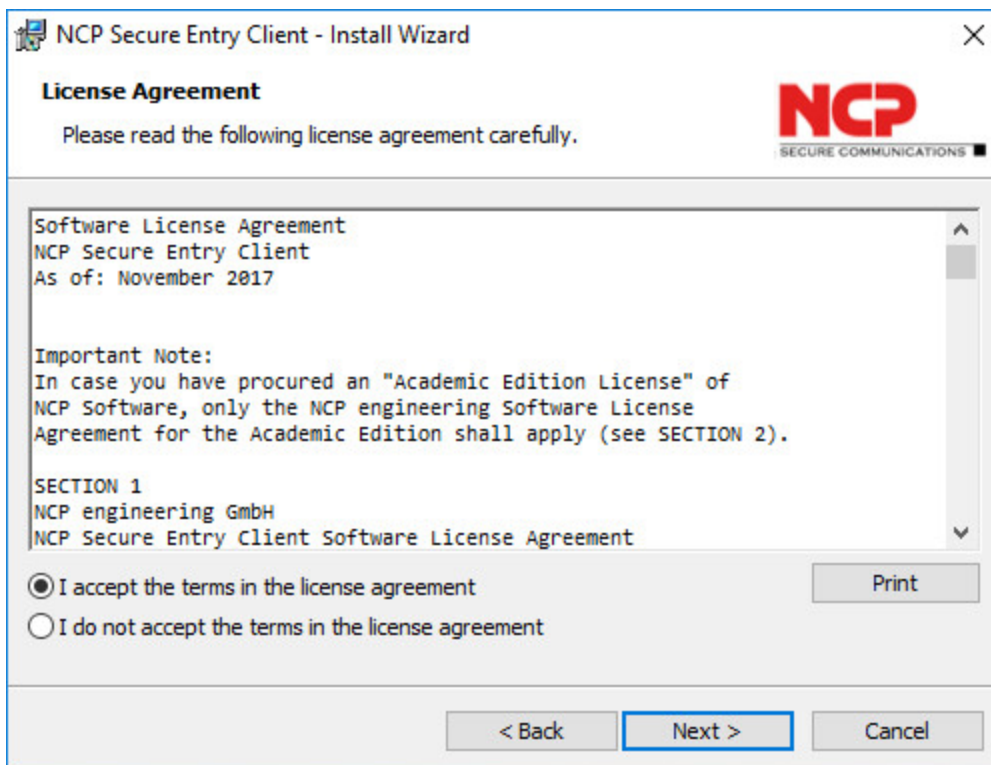
Then follow the instructions of the installation wizard.

After successful installation, restart your computer.

Trial Version

If you start the trial version, it is valid for 30 days from the time of installation and can not be used afterwards. With the start of the trial version, two VPN profiles for test connections can be created at the same time, one for IPsec with IKEv1, one with IKEv2.

Import of ncpphone.cnf and ncpphone.cfg during installation

If the files *ncpphone.cnf* or *ncpphone.cfg* are in the installation folder during the installation, they will be migrated automatically. Thus their settings are taken over and are available after the installation.

Note: *If you import a configuration file during client installation that contains stateful boot configurations of the firewall, they are displayed as active but are not yet effective at the driver level. This requires another reboot of the system.*

Adding a new VPN Profile

With the Configuration Wizard connections can be quickly made to the company network or the Internet depending on the required VPN transmission protocol. After choosing the basic settings by answering a few simple configuration questions, the VPN profile is created in the list of available VPN profiles.

Start the Client and open „Profiles...." under „Configuration" in the menu bar.
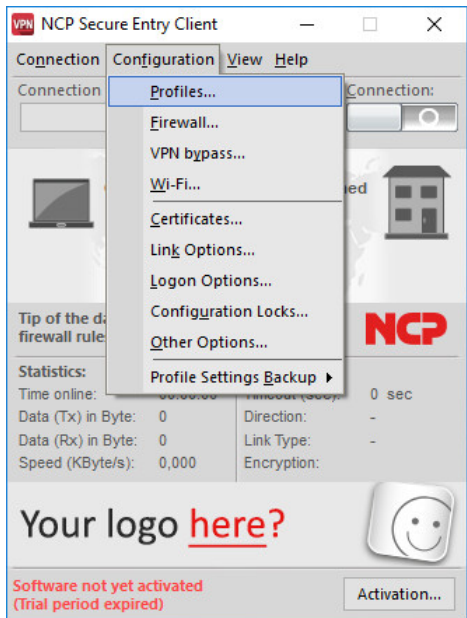
In the following window you have the possibility to add/import a new profile.
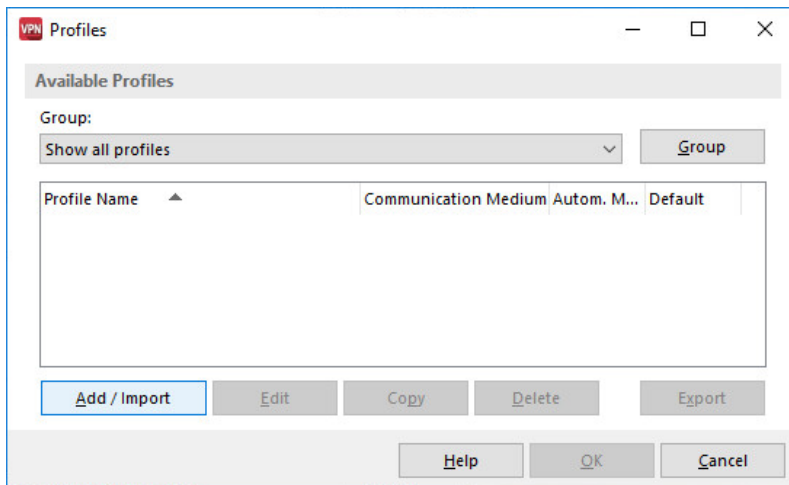
The following data are required for configuration.

Connection to the corporate network via IPsec:

- Profile Name

- Communication Medium

- Access data for Internet Service Provider (User ID, Password, Phone Number)

- VPN-Gateway selection (VPN Gateway, Tunnelsecret)

- Certificate use

- Access data for VPN Gateway (VPN User ID, VPN Password)

- Static key (Preshared Key) as long as no certificate is used (IKE ID Type, IKE ID)

Establish connection with the Internet:

- Profile Name

- Communication Medium

- Access data for Internet Service Providers (User ID, Password, Phone Number)

Alternatively an already existing VPN profile can be imported. Following formats are supported: *.ini; *.pcf; *.wgx; *.wgc

Update to Version 13

New Directory Structure with new Client

After installing Version 13 of the NCP Secure Entry Clients software, all files are no longer stored in the same directory as in previous versions (until version 11), at:

`C:\Programs\NCP\SecureClient`

In version 13 the files are stored under different paths.

Immutable files are stored exclusively under:

`C:\Programs\NCP\SecureClient`

Configuration files or files generated by the software are saved as:

`C:\ProgramData\NCP\SecureClient`

Manual Update of the Client

With a manual update, the configuration files created with the previous version are automatically moved to the directory that corresponds to the new version.

Conversion of the file structure of the client software in version 13.00

Please note the [directory structure] 21 shown below.

Check the directory paths

- All configurations that contain paths must be checked to see if they are affected by the directory change! Check all entries containing a directory and correct them if necessary.

- The placeholder `%INSTALLDIR%` already used on older clients still exists. An exception is its use in the "Determination of the paths of the certificate configuration", see below. (Concern to the [structure of the directories] 21.)

- Additionally all Windows environment variables can be used (e.g. `%ProgramFiles%`)

- In addition, all placeholders of the pathinfo.ini can be used (see below [Pathinfo.ini] 21).

Verify the paths of the certificate configuration

- If the configured P12 file exists under `% CertDir%`, only the file name will be displayed. When saving always
`%CertDir%` is prefixed.

- It is therefore recommended to place all certificates in `%CertDir%`. This completely eliminates the specification of the directory name. It is sufficient to specify the file name.

- If a file with absolute path matching `%CertDir%` is selected, it will be replaced with `%CertDir%` and only the filename will be displayed.

Directory paths of the client software from version 12.00

After standardization measures by Microsoft, only immutable files, such as binaries or resources that require execution rights, are installed under
`C:\Programs`

Therefore, starting with client versions 12.00, all files of the Secure Client software required for execution are in the directory
`C:\Programs\NCP\SecureClient`

Files that can be modified, read or recorded by the user (configuration and log files, logos and statistics) and those that are generated dynamically during the operation of the software are saved as
`C:\ProgramData`
or in the users directory under
`C:\Users`

Registry

The former registry entry InstallDir still exists and still returns the directory under `Program Files`. This is also the registry entry above which all modules currently determine the installation directory. In addition, there is now the registry entry `InstallDirData`.

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\NCP engineering GmbH\NCP Secure Client]
InstallDir     = C:\\Program Files\\NCP\\SecureClient\\
InstallDirData = C:\\ProgramData\\NCP\\SecureClient\\
```

Files with path "pathinfo.ini"

When installing the client software, the pathinfo.ini file is automatically written by the setup and created under `C:\Program Files\Company\Product`. It contains the various directories of the client software. The directories are absolute and can be read and used directly.

```
[PATHS]
BaseInstallDir      C:\Program Files\NCP\SecureClient\          Directory for committed
                                                                program files
BaseDataDir         C:\ProgramData\NCP\SecureClient\            Directory for configuration
CaCertDir           C:\ProgramData\NCP\SecureClient\cacerts     CA certificates
CertDir             C:\ProgramData\NCP\SecureClient\certs       User certificates
ArlDir              C:\ProgramData\NCP\SecureClient\arls        Zertifikatssperrlisten (ARL)
CrlDir              C:\ProgramData\NCP\SecureClient\crls        Zertifikatssperrlisten (CRL)
LogUserDir          C:\ProgramData\NCP\SecureClient\log_user    Log files of applications and service
LogDir              C:\ProgramData\NCP\SecureClient\log_system  Log files of applications and service
ConfigDir           C:\ProgramData\NCP\SecureClient\config      Configuration files
HotspotDir          C:\ProgramData\NCP\SecureClient\hotspot     Hotspot login scripts
HotspotCaCertDir    C:\ProgramData\NCP\SecureClient\hotspot\cacerts Hotspot CA certificates
```

Client Monitor

The client monitor menu contains the following sub-menus:

[Connection](#) 23
[Configuration](#) 48
[View](#) 117
[Help](#) 120

You can start the client monitor via the desktop icon. If you have chosen the installation without a desktop icon, you can start the client monitor by using the software list of your windows start menu.

Connection [Menu]

This pull-down menu contains the following menu items:

Connect / Disconnect

A connection can only be established if a profile has already been properly defined and selected; the profile to be used to establish the connection is displayed in the monitor below the menu bar.

If the function "Connect" is selected, the connection will be manually established to the destination system.

To have the link established automatically, set "Connection Mode" to the required value in the "Profile Settings / Line Management" folder.

Disconnect

A connection can be manually disconnected by clicking on "Disconnect" in the Connection pull-down menu or by clicking on the "Disconnect" switch.

Status display of the product icon

The color of the status icons change from red to green during connection.

The line under the VPN icon shows whether the firewall is active and whether the device is connected to an unknown or friendly network. If the client is in a friendly network, the line is shown in dashed lines.

(The firewall is also displayed in the graphical monitor interface 52 .)

Home Zone

The function of the Home Zone is described under the Features 200 heading.

This menu item will only appear if a Home Zone is configured in the firewall settings 54 and the firewall is active.

When the Home Zone is configured and active, it is displayed in the client interface with a symbol on the desktop (house) behind the active firewall.

The network type Home Zone was implemented to give a user access to devices on their private network (for example a network printer) while working in their home office.

Setting the Home Zone: Clicking on Set button opens the firewall so that devices can be used on the private network.

If the network parameters of the Home Zone change in the meantime, for example due to changing location, the Home Zone can be set again to overwrite the existing settings and use the current setting in the firewall. A choice of alternative Home Zones is not possible.

Deleting the Home Zone: The Delete function disables the Home Zone feature and blocks access to the private network again.

Hotspot Logon [Menu]

This menu item is only activated if the Wi-Fi manager of the client is not enabled.

If the device is in the range of a public Wi-Fi network, the hotspot logon can be used. The Client automatically searches for a hotspot and opens the website for login only with the in the client integrated browser of the current Windows operating system.

The integration of the browser into the client has ensured that the browser can not be used for other purposes.

After successful hotspot logon, the VPN connection must be established manually by using the Connect button.

Note: To use the optional hotspot detection feature, the Microsoft Edge WebView2 Runtime must be installed on the platform (seehttps://developer.microsoft.com/en-us/microsoft-edge/webview2/). If this is the case, the platform administrator must ensure that this is regularly updated to the latest version according to the platform update guidelines. When using the "Evergreen" variant of the runtime, this can be done through the Windows update mechanism.

Mobile Network Card

When a Mobile Network Card has been installed, the mobile network information field is displayed in the monitor and the Wi-Fi panel hidden. See also:

Scan for available networks 28
Enable Mobile Network 28
Enter SIM PIN 28
Change SIM PIN 29
Enter PUK 29

Scan for Available Networks / Network Scan

Immediately after the Monitor starts, the mobile network device automatically starts searching for a mobile network and, as soon as one is found, its details and the corresponding field strength are displayed in the Monitor. A new search can be initiated either by selecting the menu item or by clicking on the "Network Scan" button.

If the field strength falls below a certain level, the mobile network device automatically switches the network. When the field strength rises again, the device switches automatically back; the connection is preserved across such switches.

If a network scan is carried out when in the home country, a window with the "Home Network" is displayed - the "Home Network" is the network of the provider who supplied the SIM card. Other networks will only be displayed when outside the home country and Roaming is enabled.

 If a network scan after every start of the Monitor is not required, remove the "tick" from the check box - the default setting for this option is activated.

Enable Mobile Network

The data transmission method can also be changed manually. To do so click on the text with the desired transmission method or select this menu item. When changing the medium manually the connection will first be disconnected. The connection will then be re-established automatically, providing, in the profile settings, "Connection Mode" has been set to automatic.

Enter SIM PIN

The dialog for entering the SIM PIN is automatically displayed when a connection is to be established.

Use this menu item to also enter the SIM PIN before connection establishment.

Store SIM PIN in Configuration

When this function is selected, the SIM PIN is stored in the current 3G profile and will not need to be subsequently re-entered.

This function is not visible in the Entry Client default setting. It becomes visible and configurable for the user, when the privilege has been granted in the "Mobile Network" configuration locks , i.e. "User may save SIM PIN in configuration" has been activated.

Change SIM PIN

Changing the SIM PIN using this option updates the SIM PIN on the SIM card. This update will only be made if the current SIM PIN is entered correctly.

The SIM PIN stored in the 3G profile must be updated manually, either using the "Configuration / 3G Settings" menu item or when the the SIM PIN is requested at the start of connection establishment.

Enter PUK

After three incorrect attempts to enter the SIM PIN, the window for entering the PUK (Personal Unblocking Key), which accompanies the SIM card, is displayed. After correctly entering the PUK you are able to enter a new SIM PIN.

Connection Info

The connection information under "General" shows:

• the name of the currently selected profile

• statistical information (e.g. time online, value of timeout)

• IP addresses (VPN IP address, DNS server, VPN Endpoint)

• Security mode

• the security keys used

The connection information under "Quality of Service 77 " shows:

• the QoS groups available to the currently selected profile, which can be switched on or off as needed

• a graphical representation of the bandwidth used

Available Communication Media

This menu item opens a display of information about the communication media available and the medium currently in use. Where several communication media are used alternatingly, the Client will automatically recognise which media are currently available, each being indicated by a yellow icon. The currently active connection medium selected by the client is indicated by a check mark.

By activating the checkbox, this window will be displayed automatically if, during media detection, a connection fails. This also applies where the Client GUI has been minimized. The error will be displayed in red text behind the media type in use. Press "delete" to remove the text.

The independent appearance of the window with the connection media can be annoying with a frequent media change and new connection build-up, eg. when the Connection Mode always is chosen. Turn the automatic off in this case, by deleting the check from the checkbox.

For configuring the Automatic Media Detection, watch the parameter description for the profile settings (basic settings) of the client.

Budget Manager Statistics

The statistics show, at the current date, how much of the maximum budget has been used to date, either in hours or bytes, since the first of the current month or since the start of monitoring. Limits can be set here, in order to trigger certain actions.

Budget Manager History

Dependent on your budget settings, the budget manager history shows the total time connected and the total amount of data transferred. The budget settings are configured in "Configuration / Link Options" and can be set for each communication media separately.

Click on the show button to display the details graphically.

Certificates [View]

Certificates are created and issued by a Certification Authority (CA) (also referred to as the Issuer), using a PKI manager (software), and then either burnt onto a Smart Card (chipcard) or stored as a soft certificate (or digital certificate) in a normal file. Certificates with digital signatures can be used in the same way as a digital personal identity card.

Certificates can be created with a private key up to a length of 4096 bits.

If certficates are being used, after CHAP authentication (user ID and password) between client and VPN gateway has been used for tunnel establishment, Extended Authentication is carried out using certificates stored at the client and the VPN gateway. In this process, "Extended Authentication" together with negotiation of the session key for the previously selected encryption method are carried out.

Note for Extended Authentication 185 configuration options under Identities 183.

View Issuer Certificate

The Issuer Certificate (also referred to as a CA Certificate) can only be viewed if it is contained in the User Certificate; enter the User Certificate's PIN to display it.

View Issuer Certificate enables you to review which values were used to create the certificate, e.g. unique e-mail address.

General

The General display shows information about certificate user and issuer (these are identical for an Issuer Certificate), as well as the serial number, details about duration of validity, and the fingerprint.

Certification Authority (CA): The issuer and user of an Issuer Certificate are normally identical (self-signed certificate). The issuer of the issuer certificate has to be identical to the issuer of the user certificate (see View User Certtificate).

Serial Number: The serial number of the certificate is compared with serial numbers maintained in the Certification Authority's certificate revocation list(CRL).

Valid to/from: The validity of a certificates is limited. Normally the validity of an Issuer (Root) Certificate is longer than the validity of a User Certificate. Upon expiry of the validity of the Issuer Certificate, the validity of any User Certificate from the same CA expires as well.

Fingerprint: = hash value. The signature of the certificate is the hash value encrypted with the private key of the CA.

Extensions

Certificates can contain extensions. These are used to link additional attributes with users or public keys that are required for the administration and operation of the certification hierarchy and the revocation lists. In principle, certificates can contain any number of extensions, including those that are privately defined. The certificate extensions are written into the certificate by the issuing certification authority.

Following extensions are relevant for the Secure Client and the Secure Server:
• keyUsage
• extendedKeyUsage
• subjectKeyIdentifier
• authorityKeyIdentifier
• Certificate Distribution Point (CDP)

keyUsage

If the KeyUsage extension is contained in an incoming certificate, then it will be verified. The following KeyUsage bits are accepted. If one of the bits is not set, then the connection will be disconnected:

• Digital Signature
• Key Encipherment (keytransport, key management)
• Key Agreement (key exchange process)

extendedKeyUsage

If the extendedKeyUsage extension is present in an incoming User Certificate, then the Client checks whether the defined extended usage is "SSL Server Authentication". If the incoming certificate is not intended for server authentication, then the connection will be refused. If this extension is not present in the certificate, then this will be ignored.

Note that SSL Server Authentication is direction dependent, i.e. the initiator of tunnel establishment checks the incoming certificate of the remote party, if the extendedKeyUsage extension is present, then the intended usage must contain "SSL Server Authentication".

subjectKeyIdentifier / authorityKeyIdentifier

A key identifier is an additional ID (hash value) to the CA name on a certificate. The authoritykeyidentifier (SHA1 hash over the issuer's public key) on the incoming certificate must agree with the subjectKeyIdentifier (SHA1 hash over the public key of the owner) on the corresponding CA certificate. If no CA Certificate is found then the connection is rejected.

The keyidentifier designates the public key of the Certification Authority and in this way not only one, but a series of certificates if required. The use of the key identifier allows a greater flexibility for the determination of a certificate path. In addition, the certificates that possess the authoritykeyidentifier extension do not need to be revoked if the CA issues a new certificate when the key remains the same.

Certificate Distribution Point (CDP)

The URL for downloading a Certificate Revocation List(CRL) is stored in the CDP. If the CPD extension is contained in the certificate, then after the connection is set up, the CRL is downloaded via the specified URL and checked. If the system determines that the certificate is invalid then the connection is disconnected. In this process the CRL is stored in the %INSTALLDIR%\crls directory, under the common name of the CA.

View User Certificate

In order to view the User Certificate, first enter the PIN.

View User Certificate enables you to review which values have been used to create the certificate, e.g. unique e-mail address.

General

The General display shows information about certificate user and issuer (these are identical for an Issuer Certificate), as well as the serial number, details about duration of validity, and the fingerprint.

Certification Authority (CA): The issuer/CA of your User Certificate must be identical to the issuer of the CA certificate. (see View Issuer Certificate).

Serial Number: The serial number of the certificate is compared with the serial number kept in the revocation list of the Certification Authority (CRL).

Valid to/from: The validity of a certificates is limited. Normally the validity of an Issuer (Root) Certificate is longer than the validity of a User Certificate. When the validity expires the functionality of the certificate is also lost.

Fingerprint: = hash value. The signature of the certificate is the hash value encrypted with the private key of the CA.

Extensions

Certificates can contain extensions. These are used to link additional attributes with users or public keys that are required for the administration and operation of the certification hierarchy and the revocation lists. In principle, certificates can contain any number of extensions, including those that are privately defined. The certificate extensions are written into the certificate by the issuing certification authority.

Following extensions are relevant for Secure Client and the Secure Server:
• keyUsage
• extendedKeyUsage
• subjectKeyIdentifier
• authorityKeyIdentifier
• Certificate Distribution Point (CDP)

keyUsage

If the KeyUsage extension is contained in an incoming certificate, then it will be verified. The following KeyUsage bits are accepted:
• Digital Signature
• Key Encipherment (keytransport, key management)
• Key Agreement (key exchange process)
If one of the bits is not set, then the connection will be disconnected.

extendedKeyUsage

If the extendedKeyUsage extension is present in an incoming User Certificate, then the Client checks whether the defined extended usage is "SSL Server Authentication". If the incoming certificate is not

intended for server authentication, then the connection will be refused. If this extension is not present in the certificate, then this will be ignored.

Note that SSL Server Authentication is direction dependent, i.e. the initiator of tunnel establishment checks the incoming certificate of the remote party, if the extendedKeyUsage extension is present, then the intended usage must contain "SSL Server Authentication".

subjectKeyIdentifier / authorityKeyIdentifier

A key identifier is an additional ID (hash value) to the CA name on a certificate. The authoritykeyidentifier (SHA1 hash over the issuer's public key) on the incoming certificate must agree with the subjectKeyIdentifier (SHA1 hash over the public key of the owner) on the corresponding CA certificate. If no CA Certificate is found then the connection is rejected.

The keyidentifier designates the public key of the Certification Authority and in this way not only one, but a series of certificates if required. The use of the key identifier allows a greater flexibility for the determination of a certificate path. In addition, the certificates that possess the authoritykeyidentifier extension do not need to be revoked if the CA issues a new certificate when the key remains the same.

Certificate Distribution Point (CDP)

The URL for downloading a Certificate Revocation List(CRL) is stored in the CDP. If the CPD extension is contained in the certificate, then after the connection is set up, the CRL is downloaded via the specified URL and checked. If the system determines that the certificate is invalid then the connection is disconnected. In this process the CRL is stored in the %INSTALLDIR%\crls directory, under the common name of the CA.

View Incoming Certificate

View the certificate that was transmitted from the remote side (Secure Server) as part of the SSL negotiation. You can see, for example, whether you have accepted the issuer displayed here in the list of your CA certificates (see below).

If the incoming User Certificate is from one of the CAs not known in the "Display CA Certificates" list, or if it does not match with the Root Certificate in the p12 file, then the connection will not be established.

General

The General display shows information about certificate user and issuer (these are identical for an Issuer Certificate), as well as the serial number, details about duration of validity, and the fingerprint.

Extensions

Certificates can contain extensions. These are used to link additional attributes with users or public keys that are required for the administration and operation of the certification hierarchy and the revocation lists. In principle, certificates can contain any number of extensions, including those that are privately defined. The certificate extensions are written into the certificate by the issuing certification authority.

Following extensions are relevant for Secure Client and the Secure Server:
• keyUsage
• extendedKeyUsage
• subjectKeyIdentifier
• authorityKeyIdentifier
• Certificate Distribution Point (CDP)

KeyUsage

If the KeyUsage extension is contained in an incoming certificate, then it will be verified. The following KeyUsage bits are accepted. If one of the bits is not set, then the connection will be disconnected:
• Digital Signature
• Key Encipherment (keytransport, key management)
• Key Agreement (key exchange process)

extendedKeyUsage

If the extendedKeyUsage extension is present in an incoming User Certificate, then Client checks whether the defined extended usage is "SSL Server Authentication". If the incoming certificate is not intended for server authentication, then the connection will be refused. If this extension is not present in the certificate, then this will be ignored.

Note that SSL Server Authentication is direction dependent, i.e. the initiator of tunnel establishment checks the incoming certificate of the remote party, if the extendedKeyUsage extension is present, then the intended usage must contain "SSL Server Authentication".

subjectKeyIdentifier / authorityKeyIdentifier

A key identifier is an additional ID (hash value) to the CA name on a certificate. The authoritykeyidentifier (SHA1 hash over the issuer's public key) on the incoming certificate must agree with the subjectKeyIdentifier (SHA1 hash over the public key of the owner) on the corresponding CA certificate. If no CA Certificate is found then the connection is rejected.

The keyidentifier designates the public key of the Certification Authority and in this way not only one, but a series of certificates if required. The use of the key identifier allows a greater flexibility for the determination of a certificate path. In addition, the certificates that possess the authoritykeyidentifier extension do not need to be revoked if the CA issues a new certificate when the key remains the same.

Certificate Distribution Point (CDP)

The URL for downloading a Certificate Revocation List(CRL) is stored in the CDP. If the CPD extension is contained in the certificate, then after the connection is set up, the CRL is downloaded via the specified URL and checked. If the system determines that the certificate is invalid then the connection is disconnected. In this process the CRL is stored in the %INSTALLDIR%\crls directory, under the common name of the CA.

HTTP Proxy for CRL Download

A proxy for the CRL download can be configured via HTTP in the ncppki.conf file in the "HttpProxy" group:

```
[HttpProxy]

ProxyHost = xxx.xxx.xxx.xxx

#IP address of the proxy server for CRL download via HTTP

ProxyPort = 80

#Port of the proxy server for CRL download via HTTP

ProxyUser = xyz

#Username of the proxy server for CRL download via HTTP

ProxyPw = xxxx

#Password of the proxy server for CRL download via HTTP
```

CRL and ARL Checks

The client is also capable of checking the following revocation lists:

• Certificate Revocation List (CRL)

• Authority Revocation List (ARL)

The CRLs and ARLs must be copied to the respective (i.e. "\CRL" or "\ARL") subdirectories in the installation directory.

View CA Certificates

Multiple issuer certificates are supported with the client software (Multiple CA Support). For this, the issuer certificates must be collected in the installation directory under "cacerts". In the client monitor the list of CA certificates read-in is displayed under this menu item.

If a certificate of a remote system is received, then the client determines the issuer, then searches for the issuer in the CA certificates.

If no CA Certificate matches, then the connection will not be established (No Root Certificate found!).

General

The General display shows information about certificate user and issuer (these are identical for an Issuer Certificate), as well as the serial number, details about duration of validity, and the fingerprint.

Extensions

Certificates can contain extensions. These are used to link additional attributes with users or public keys that are required for the administration and operation of the certification hierarchy and the revocation lists. In principle, certificates can contain any number of extensions, including those that are privately defined. The certificate extensions are written into the certificate by the issuing certification authority.

Following extensions are relevant for Secure Client and the Secure Server:
• KeyUsage
• extendedKeyUsage
• subjectKeyIdentifier
• authorityKeyIdentifier
• Certificate Distribution Point (CDP)

KeyUsage

If the KeyUsage extension is contained in an incoming certificate, then it will be verified. The following KeyUsage bits are accepted. If one of the bits is not set, then the connection will be disconnected:
• Digital Signature
• Key Encipherment (keytransport, key management)
• Key Agreement (key exchange process)

extendedKeyUsage

If the extendedKeyUsage extension is present in an incoming User Certificate, then the Client checks whether the defined extended usage is "SSL Server Authentication". If the incoming certificate is not intended for server authentication, then the connection will be refused. If this extension is not present in the certificate, then this will be ignored.

Note that SSL Server Authentication is direction dependent, i.e. the initiator of tunnel establishment checks the incoming certificate of the remote party, if the extendedKeyUsage extension is present, then the intended usage must contain "SSL Server Authentication".

subjectKeyIdentifier / authorityKeyIdentifier

A key identifier is an additional ID (hash value) to the CA name on a certificate. The authoritykeyidentifier (SHA1 hash over the issuer's public key) on the incoming certificate must agree with the subjectKeyIdentifier (SHA1 hash over the public key of the owner) on the corresponding CA certificate. If no CA Certificate is found then the connection is rejected.

The keyidentifier designates the public key of the Certification Authority and in this way not only one, but a series of certificates if required. The use of the key identifier allows a greater flexibility for the determination of a certificate path. In addition, the certificates that possess the authoritykeyidentifier extension do not need to be revoked if the CA issues a new certificate when the key remains the same.

Certificate Distribution Point (CDP)

The URL for downloading a Certificate Revocation List(CRL) is stored in the CDP. If the CPD extension is contained in the certificate, then after the connection is set up, the CRL is downloaded via the specified URL and checked. If the system determines that the certificate is invalid then the connection is disconnected. In this process the CRL is stored in the %INSTALLDIR%\crls directory, under the common name of the CA.

Computer Certificate (View)

View Hardware Certificate enables you to review which values have been used to create the certificate, e.g. unique e-mail address.

General

The General display shows information about certificate user and issuer (these are identical for an Issuer Certificate), as well as the serial number, details about duration of validity, and the fingerprint.

Certification Authority (CA): The issuer of your User Certificate has to be identical with the issuer of the CA certificate. (see View Issuer Certificate).

Serial Number: The serial number of the certificate is compared with the serial number kept in the revocation list of the Certification Authority (CRL).

Validity: The validity of a certificates is limited. Normally the validity of an Issuer (Root) Certificate is longer than the validity of a hardware Certificate. When the validity expires the functionality of the certificate is also lost.

Fingerprint: = hash value. The hash value is the signature of the certificate. The hash value is encrypted with the private key of the CA.

Extensions

Certificates can contain extensions. These are used to link additional attributes with users or public keys that are required for the administration and operation of the certification hierarchy and the revocation lists. In principle, certificates can contain any number of extensions, including those that are privately defined. The certificate extensions are written into the certificate by the issuing certification authority.

Following extensions are relevant for Secure Client and the Secure Server:
• KeyUsage
• extendedKeyUsage
• subjectKeyIdentifier
• authorityKeyIdentifier
• Certificate Distribution Point (CDP)

KeyUsage

If the KeyUsage extension is contained in an incoming certificate, then it will be verified. The following KeyUsage bits are accepted:
• Digital Signature
• Key Encipherment (keytransport, key management)
• Key Agreement (key exchange process)
If one of the bits is not set, then the connection will be disconnected.

extendedKeyUsage

If the extendedKeyUsage extension is present in an incoming User Certificate, then the Secure Client checks whether the defined extended usage is "SSL Server Authentication". If the incoming certificate is not intended for server authentication, then the connection will be refused. If this extension is not present in the certificate, then this will be ignored.

Note that SSL Server Authentication is direction dependent, i.e. the initiator of tunnel establishment checks the incoming certificate of the remote party, if the extendedKeyUsage extension is present, then the intended usage must contain "SSL Server Authentication".

subjectKeyIdentifier / authorityKeyIdentifier

A key identifier is an additional ID (hash value) to the CA name on a certificate. The authoritykeyidentifier (SHA1 hash over the issuer's public key) on the incoming certificate must agree with the subjectKeyIdentifier (SHA1 hash over the public key of the owner) on the corresponding CA certificate. If no CA Certificate is found then the connection is rejected.

The keyidentifier designates the public key of the Certification Authority and in this way not only one, but a series of certificates if required. The use of the key identifier allows a greater flexibility for the determination of a certificate path. In addition, the certificates that possess the authoritykeyidentifier extension do not need to be revoked if the CA issues a new certificate when the key remains the same.

Certificate Distribution Point (CDP)

The URL for downloading a Certificate Revocation List(CRL) is stored in the CDP. If the CPD extension is contained in the certificate, then after the connection is set up, the CRL is downloaded via the specified URL and checked. If the system determines that the certificate is invalid then the connection is disconnected. In this process the CRL is stored in the %INSTALLDIR%\crls directory, under the common name of the CA.

Enter PIN

The PIN can be entered before establishing a connection but after the Monitor has been started. If a connection requiring a certificate is to be established at a later time, then the PIN entry can be omitted - unless the configuration for the certificate demands it.

If you have selected the menu item "Connection / Enter PIN", then the PIN (at least 4 digits) can be entered in the open entry field, and confirmed with "OK".

If the PIN has not been entered before connection establishment, the PIN entry dialog is started, at the latest, when the first connection requiring the use of a certificate is to be established to a destination . After that, the PIN entry can be omitted in the case of repeated manual connection establishment, if this has been configured.

If the PIN has been entered correctly, this is indicated in the monitor interface by a green PIN symbol.

A connection can only be established after correct entry of the PIN.

Safeguarding PIN Use

If you activate the function "PIN request at each connection" in the certificate configuration, then the PIN can no longer be entered via the "Enter PIN" Monitor menu option. For this reason, the menu option "Enter PIN" is automatically switched off (grayed out). This ensures that the PIN will only be queried and can only be entered directly before the connection is set-up.

Activate this function to prevent an unauthorized user from setting up an unauthorized connection when the PIN has already been entered.

Likewise, if the "Change PIN" function has been activated, the PIN that has already been requested in connection with other functions is no longer used - i.e. when setting up a connection, or in the "Enter PIN" connection menu. Instead you can always select the menu option "Change PIN" and the new PIN will be automatically reset immediately after the change.

This ensures that when configuring "PIN query at every connection set up" on an unauthorized Secure Client Monitor, a PIN entered previously by an unauthorized user cannot be used at anytime to establish a connection.

The policies for PIN entry can be specified in the main menu under "Configuration / Certificates". These policies must be observed when the PIN is changed.

Reset PIN

This menu item is active only when the PIN has been entered correctly, i. e. the certificate is used for the connection to be established.

If the PIN is reset, this certificate can no longer be used to establish a connection, until the correct PIN is entered again.

Change PIN

The PIN for a smartcard/token or for a soft certificate can be changed under the menu item "Change PIN", providing the correct PIN number has previously been entered.

Then enter your new PIN and confirm it by repeating it in the last entry field. With a click on "OK" you have changed your PIN.

PIN policies that need to be complied with are displayed under the entry field. They can be set in the main menu under "Certificate - PIN Policies".

Unlock Parameters

This menu item will only be displayed if configuration locks have been configured by your system administrator.

Your system administrator may have purposely hidden and locked various profile parameter folders or menu items. These will no longer be visible and therefore cannot be modified under normal circumstances.

In order to display these parameters, select this menu item. After correctly entering User ID and Password, the configurations will be unlocked, and changes can now be made;

The Connection menu item changes to "Lock Configuration Locks" when the parameters are unlocked.

Exit

If the connection is already disconnected, clicking this menu item or the close button quits the client. If a connection is currently established, the monitor can be quitted after clicking on this menu item or on the close button. Note, however, that an existing connection will not be automatically disconnected. If the potentially chargeable connection is to remain established even though the monitor is being quitted, confirmation will be requested.

Upon selecting "No" your desktop will not display any icon and you will not be notified that the link is active and that charges may be incurred. In such a case, the monitor of the client must be restarted in order to be able to disconnect correctly.

Configuration [Menu]

This pull-down menu contains the following menu items:

Using this menu item, you can configure all the parameter needed for working with the Secure Client. Specifically this means creating profiles, the IPsec configuration, as well as selection of the communication medium.

In addition you can configure precisely how certificates should be used and how the Budget Manager (under "Link Options") should work.

Profiles [Configuration]

Configuring Client Profiles

After the software is first installed there are no profiles setup in the client software, and hence the "New Profile Wizard" is opened which guides you through profile configuration. The profile created becomes the first in the IPsec client software.

Add / Import

Click on this button to start a wizard which helps you to either configure a new profile or import an existing profile.

The client supports different types of import files (*.ini).

The desired profile settings can be created by the remote gateway or edited manually. Sample import files IMPORT_D.txt and IMPORT_E.txt are stored in the installation directory. The sample files include syntax and parameter values.

Export

Click on this button to start a wizard which helps you to export the selected profile.

See also:

Profile Settings 50
Profile Groups 51

Profile Settings

Profile Groups

You can sort these profiles in the list of all profiles by name, by communication medium, and (in case of a dial-up connection) by phone number.

Should the list of profiles be too long for sorting, profiles can also be divided up into groups. Click on "Group" above the phone noumber display to open the group configuration.

Click on "Add" to add a new group to the column on the left, which you can then name if you wish to group together profiles of that type.

Select profiles from the right-hand column to add them to the new group shown in the column on the left. You can associate profiles with multiple groups where required.

Click on "Edit" to edit the name of the group. Click on "Delete" to remove the group currently displayed, and the relevant profile associations. The profiles themselves will not be deleted.

Group Display

You can now display all profiles, or alternatively only those profiles that have been associated with a selected profile group.

An info text is displayed on the user interface of the monitor in the profile selection area, where you can also choose to display all profiles, or just those associated with a particular group.

Firewall [Configuration]

All Firewall mechanisms are optimized for remote access applications and are activated during the computer's startup process, hence they are active as soon as the computer is ready for use.

If the Firewall is active, its state is reported to the Windows Security Center or the Maintenance Center and can be viewed there.

This means that in contrast to VPN solutions with an autonomous firewall, the computer is protected against attacks before any actual use of the VPN.

The Firewall also offers complete protection of the end device, even if the Secure Client software is deactivated.

Note that the Firewall settings are globally valid and they are applied for all profiles.

Firewall Properties

The Firewall uses packet filtering techniques in conjunction with Stateful Packet Inspection (SPI). The Firewall checks all incoming and outgoing data packets and decides whether a packet will be forwarded or rejected, based on preconfigured rules.

Security is ensured in two ways. First, unauthorized access to data and resources in the central data network is prevented. Second, the respective status of existing connections is monitored via Stateful Inspection. Further, the Firewall can detect whether a connection has opened "spawned connections" - as is the case with FTP or Netmeeting for example - whose packets likewise must be forwarded. If a rule is defined which permits access for an outgoing connection, then the rule automatically applies to all the corresponding return packets. For the communication partner a stateful inspection connection is represented as a direct line, which can only be used for an exchange of data that corresponds to the agreed rules.

The Firewall rules can be configured dynamically, i.e. it is not necessary to stop the software or restart the computer.

The Firewall settings in the Secure Client Monitor's Configuration Menu enable a very precise specification of Firewall filtering rules. They have a global effect.

The Symbol of the Firewall

Depending on the firewall configuration, the firewall icon in the GUI and the taskbar will be different:

If the user's computer is establishing a connection in a friendly network, the protective shield of the firewall symbol is displayed with a green border directed to the remote station:

(The firewall is also displayed with the product icon 24 .)

This means that regardless of the currently selected profile, the rules of the extended Firewall settings are always worked through first, before the Firewall rules are applied.

A combination of the global and link based Firewall can be effective in certain scenarios. Usually, the global setting possibilities should be able to cover virtually all requirements.

Please note that the link-based Firewall settings take priority over the global Firewall settings at activation.

For instance if the Link Firewall is set to "Always" and "Only allow communication in the tunnel", then in spite of global configuration rules that may possibly be different, only one tunnel can be set up for communication. All other traffic will be rejected by the Link Firewall.

Configuration of the Firewall Settings

The filter rules of the Firewall can be defined application-based as well as (additionally) address-oriented, relative to friendly / unknown networks.

Refer also to:

Basic Settings with Default Configuration 54
Rules Table 57
Friendly Networks 62
Options 69
Logging 74

Basic Settings with Default Configuration

Default Configuration in the Basic Settings

When the Secure Client software is updated, any previous Firewall settings remain in operation.

When the Secure Client is installed for the first time on a machine, i.e. a new installation, the Firewall will not yet be enabled after the first start of the Secure Client

Enable Firewall

To enable the firewall, select the Secure Client Monitor's "Configuration / Firewall" menu item, then, in the "Basic Settings" displayed, click on the "Enable Firewall" option.

As soon as the Firewall is enabled, a symbol (protection shield) is displayed in the the Secure Client Monitor indicating that all IP communication in the network (LAN, printers, etc.) is blocked, regardless of whether it is IPv4 or IPv6 or whether incoming or outgoing. This happens when no explicit Firewall rules have been created or enabled.

Rules for Use during Test Connections

If, during the installation of the software, the opportunity is taken to setup a test connection (Test Connection IPsec IKEv1 or Test Connection IPsec IKEv2), a connection can be established even when the Firewall is enabled by inserting the predefined firewall rule "NCP rules for test connection".

This is a quick way to test the functionality of the firewall.

Selecting and Editing a Rule

In the following, editing is illustrated using predefined rules.

• Select the required rule (in the following, predefined rules for test connections are described).

• Click on "Install". This causes four individual rules to be inserted into the rules list and these are all immediately enabled.

• the rules are acted on by the Firewall as soon as the Firewall settings are closed by pressing "OK". Pressing the "Apply" button stores the rules but does not close the Firewall display.

If all the rules for the test connection are enabled and the Firewall symbol (protection shield) is displayed in the Monitor after the Firewall settings are closed, then the "Test Connection" connection profile can be used to establish a connection to the NCP VPN gateway.

Additional Rules permit the defined establishment of the tunnel

The predefined "NCP rules for test connection" inserts the following individual rules into the firewall:
• NCP DNS
• NCP Web Browser
• NCP FTP
• NCP Ping (IPv4)

The following command is always enabled in the default configuration:

• Permit IPsec protocol (ESP, UDP 500) and VPN Path Finder (TCP 443)

enables VPN tunnel establishment globally.

The following protocols and ports required for the IPsec tunnel establishment are enabled by an automatically generated filter:

• IP protocol 50 (ESP)
• UDP 4500 (NAT-T)
• UDP 67 (DHCPS)
• UDP 68 (DHCPC)
• TCP 443 (VPN Path Finder, if configured)
Activating this function avoids having to configure individual rules for the respective VPN variants.

Note: this only enables tunnel establishment. If there are no other rules defined for the VPN network and that enable communication in the tunnel, data cannot be transferred through the tunnel.

Other predefined Firewall rules can be selected as necessary, inserted into the list of Firewall rules using the "Insert" button, and then edited.

Rule(s) for DNS requests

The Test Connection profile, automatically created during the installation, contains a Tunnel Endpoint defined with the DNS name "vpntest.ncp-e.com". Establishment of a tunnel will fail if the NCP DNS Firewall rule is not enabled, as the attempt to contact the DNS name server to resolve the DNS name "vpntest.ncp-e.com" will fail.

In order to enable name resolution and permit a DNS request to pass through the firewall, there are also the following predefined Firewall rules available that can be inserted and used unmodified:

• DNS request (IPv4)

• DNS request (IPv6)

• DNS request (unknown network)

Rules for Web Browsers

The NCP rule for web browsers only allows access to the web server via a VPN tunnel to the VPN test gateway (remote IP address 172.16.12.100). In addition, only HTTP (remote port 80) web sites are supported, web sites with server verification (remote port HTTPS, 443) are not supported. The rule only applies to IPv4 addresses

An additional rule for Internet access via web browser allows access via all networks, also allows HTTPS and applies for both IPv4 and IPv6.

Rule for FTP

The NCP rule for FTP access only allows the connection via a VPN tunnel to the NCP test gateway (remote IP Address 172.16.12.100) via remote ports 20 and 21.

Rule for Remote Desktop

The Firewall rules that allow access to a remote computer (RDP access) is preconfigured for remote port 3389.

Allow all Outgoing Connections

Using this rule allows all outgoing connections from this computer, both via a VPN and in known or unknown networks.

Allow All Connections in Friendly Network

Using this rule, all connections from and to the computer to and from a friendly network, respectively, are allowed. In this case access to the computer from the friendly network is also allowed.

Allow all Connections in VPN

Using this rule all connections via the VPN are allowed. In this case access to the computer from the VPN is also allowed!

Permit IPsec protocol and VPN Path Finder

The set up of VPN connections via the "Options" tab can be enabled globally.

The following protocols required for tunnel establishment are enabled, for IPsec and the VPN Path Finder technology, by an automatically generated filter:

• IP-Protokoll 50 (ESP)
• UDP 4500 (NAT-T)
• UDP 67 (DHCPS)
• UDP 68 (DHCPC)
• TCP 443 (VPN Path Finder, if configured)

Activating this function avoids having to configure individual rules for the respective VPN variants.

Note: this only enables tunnel establishment. If there are no other rules defined for the VPN network and that enable communication in the tunnel, data cannot be transferred through the tunnel.

Rules Table
Creating and Editing a Firewall Rule

Rules are created and edited using the buttons displayed below. Click on "New" or "Copy" to create a Firewall rule, "Edit" to modify a rule or "Delete" to delete a rule.

Edit mode can be switched on either by a double click on the parameter field to be edited or on the rule in the table to be edited.

Use the tab key to jump from field to field in the rule being edited.

In the rule table, all Firewall rules are displayed that have been selected from the predefined list or have been newly created.

Rules that have been inserted from the predefined list are automatically enabled. Newly created rules must be enabled manually.

Click on a column heading or symbol to sort the listed rules accordingly.

If a rule is added or changed after the Firewall configuration is opened, the "Apply" button is activated. Use "Apply" to transfer the new settings in their entirety in the firewall's rules database, rather than leaving the Firewall configuration by pressing "OK" and then having to re-open the Firewall configuration.

The column headings and symbols of the rules table, from left to right, are:

Enable

Rules that have been inserted from the predefined list are automatically enabled. Newly created rules must be enabled manually.

A rule is only applied to a data packet after that rule has been enabled.

Name

A rule's name can be changed at any time.

Direction

Use direction to specify whether a rule applies for incoming or outgoing data packets. If the direction is set to outgoing, stateful inspection is used. Stateful inspection is only used for UDP and TCP protocols.

"Incoming" should only be set when connections should be established from the remote side (e.g. for administrator access).

The "bidirectional" setting should only be used when Stateful Inspection is not being used, e.g. for ICMP protocol (by a ping).

Action

Action is normally always set to "allow".

Only in special cases should action be set to "drop"; such as when in a rule the admissibility for an IP address range or port range has been defined and a second rule defines, for example that an individual address or port should be denied inside that first range. In such a case the second rule for the individual address or port would be set to "drop".

VPN / Friendly Network / Unknown Network

When creating a rule, at first it is not assigned to any network.

Unknown Networks

- are all networks (IP network interfaces) that can neither be allocated to a friendly network nor to a VPN.These include for example connections via the Microsoft remote data transmission network, direct or unencrypted connections with the integrated dialer of the Client, as well as hotspot Wi-Fi connections.

If this rule is to apply for unknown networks, this option has to be activated.

Friendly Networks

- are defined in the tab of the same name in the "Firewall settings" window. If a rule applies to known networks, this option has to be activated.

VPN Networks

- are all IPsec connections in the established condition. Apart from that, this group covers all encrypted direct dial-in connections via the Client's integrated dialer. If this rule is to apply for VPN networks this option has to be activated.

Protocol

Select the corresponding protocol, dependent on the application or type of connection: TCP, UDP, ICMP, GRE, ESP, AH, IGRP, RSVP, IPv6 or IPv4, ICMPv6, all

Application

Click on the directory symbol to browse to the appropriate directory and select the application that will be used to create the connection. Only this locally installed application, for example Internet Explorer, can communicate.

Automatic Connection Establishment

Not active in the default settings

(only used in dial-up type connections such as mobile networks with automatic connection establishment in the current profile)

This option is only appropriate when, in the connection profile "Line Management" parameter folder, "Connection Mode" is set to "automatic". When this function is set for a particular rule, automatic

connection establishment does not take place for the data packets defined by the rule, however, it does for other data packets.

only valid at inactive VPN connection

Select this option for the associated rule when, for example, an Internet connection is not allowed to be established over an already established VPN connection, but allowed when in an unknown network. In addition, this rule must be used for the "unknown network", i.e. the rule must allow access to the unknown network.

Local Ports and IP Addresses

Those data packets will be allowed through the firewall, whose source address matches the address or address range defined in "Local IP addresses".

Similarly for IP ports. Data packets that are to be allowed through the Firewall must have a source port corresponding to a port or ports defined here.

IP Addresses

Under the Local IP address field(s), define which IP address(s) of outgoing packets should be allowed by the firewall. The following entries are valid:

anyv4: allows communication with any IPv4 address from the local side (source address), without restriction.

anyv6: allows communication with any IPv6 address from the local side (source address), without restriction.

specific address: individual addresses can be entered, one under the next, after pressing the "+" button, (different protocol version addresses can also be mixed in the list).

The notations are:

123.10.62.1 / 32 (for IPv4)

fd00:6e93:5063:37de:12:16:8005:7a / 128 (for IPv6)

address range: two methods are available for representing address ranges.

For IPv4, 32-, 24-, 16-, 8- or other bit masks between 1 and 32 can represent a range to be masked out:

123.10.62.1 / 24 represents the range (from - to)

123.10.62.0 - 123.10.62.255

In the same way, IPv6 address with bit masks between 1 and 128 can represent an area to be masked out:

fd00:6e93:5063:37de:12:2c35:987c:2450 / 64 represent the range (from - to) fd00:6e93:5063:37de:12)

fd00:6e93:5063:37de:: - ...

Ports

Under the Local Port entry or entries, define which port(s) can be used on the local system. The following entries are valid:

any: allows communication via all source ports for outgoing packets and all destination ports for incoming packets.

specific port: the ability to define a specific port can be useful when a machine must make a server service available (e.g. Remote Desktop on port: 3389).

port range: can be used when multiple ports are required for a particular rule (e.g. FTP port: 20/21).

Remote Ports and IP Addresses

Those data packets will be allowed through the firewall, whose source address matches the address or address range defined in "Remote IP addresses".

Similarly for IP ports. Data packets that are to be allowed through the Firewall must have a destination port corresponding to a port or ports defined here.

IP Addresses

Under the Remote IP address entry, define which remote IP addresses the system should be allowed to communicate with. The following entries are valid:

anyv4: allows communication with all IPv4 addresses of the remote site, without restriction.

anyv6: allows communication with all IPv6 addresses of the remote site, without restriction.

specific address: individual addresses can be entered, one under the next, after pressing the "+" button, (different protocol version addresses can also be mixed in the list).

The notations are:

123.10.62.1 / 32 (for IPv4)

fd00:6e93:5063:37de:12:16:8005:7a / 128 (for IPv6)

address range: two methods are available for representing address ranges.

For IPv4, 32-, 24-, 16-, 8- or other bit masks between 1 and 32 can represent a range to be masked out:

123.10.62.1 / 24 represents the range (from - to) 123.10.62.0 - 123.10.62.255

In the same way, IPv6 address with bit masks between 1 and 128 can represent an area to be masked out:

fd00:6e93:5063:37de:12:2c35:987c:2450 / 64 represent the range (from - to) fd00:6e93:5063:37de:12

fd00:6e93:5063:37de:: - ...

Ports

Under the Remote Port field(s) define which port(s) on the remote system may be accessed. The following entries are valid:

any: sets no restrictions regarding the destination port for outgoing or source port for incoming packets.

specific port: allows communication only to the defined port when this is the destination port in outgoing or from the defined port when this is the source port for incoming packets. If, for example, a rule should enable Telnet to another system port 23 has to be entered here.

---

port range: can be used when multiple ports are required for a particular rule (e.g. FTP port: 20/21).

Friendly Networks

If, in the rules table, you have defined that a rule is to be applied to connections with friendly network, then this rule is always used if a network can be identified as a friendly network according to the criteria entered here, e.g. the LAN adapter is in a friendly network.

What constitutes a friendly net is defined centrally by the administrator. This can be configured manually or by using the automation facility of friendly network detection.

The manual definition of a known network by the administrator and the automatic detection of a known network via friendly net detection are not mutually exclusive, rather they can be used concurrently and they can be configured via the "Manual" and "Automatic" tabs.

A Friendly Net is signaled in the monitor by the firewall icon, the border of which turns half green when the client connects to a friendly net:

In addition, selected actions can be started as soon as the Client detects a friendly net or when friendly net detection fails.

See the following menu items:

Manual Configuration of Friendly Networks

The Client's LAN adapter is considered to be located in the friendly net when:

IP Network and Net Mask

• the IP address of the LAN adapter originates from the specified network range. If, for example, the IP network 192.168.254.0 is specified with the mask 255.255.255.0, then the address 192.168.254.10 would be assigned to the friendly network.

DHCP Server

• the IP address has been assigned by the DHCP server that has the IP address specified here.

The more of these conditions that are fulfilled, the more precise the verification that a friendly network is involved.

The allocation of an adapter to unknown or friendly network is automatically logged in the log window of the Secure Client Monitor and in the Firewall's log file (see: Logging).

Automatic Detection of Friendly Networks

Automatic detection of friendly networks requires a Friendly Net Detection Server (FNDS), i.e. a software component installed in the network defined as friendly network, and which is reachable by its IP address.

IP address automatically assigned by DHCP

With this option the client automatically receives the IP address of the FND server by DHCP.

A prerequisite is that a DHCP negotiation is triggered by the client's LAN adapter, in order to automatically receive the IP address for the LAN adapter from the DHCP server. (This is the operating systems default configuration of the network settings.)

A DHCP default option has to be added to the DHCP server of the corporate network. This DHCP default option has to contain code 159 and the IP address of the FND server that is then automatically distributed during DHCP negotiation.

IP address for friendly network detection service

If the IP address of the FND server is to be predefined, enter it in this field.

To increase reliability, the IP address of a second FND server can be entered after the first IP address, separated by a comma, semi-colon or blank. The IP address of the first available FND server will be selected automatically for friendly net detection.

User ID, Password (FNDS)

The Friendly Net Detection Server is authenticated using MD5 or TLS. The User ID (required for MD5 and TLS) and Password (required only for MD5) entered here must agree with those that have been stored on the FNDS.

Friendly Net Detection using TLS

If the friendly net is to be detected using TLS, including authentication using the Issuer Certificate fingerprint, this Issuer Certificate has to be located in the client's "CaCerts" directory, and its fingerprint must agree with the fingerprint configured here.

Incoming Certificate's Subject (User)

The incoming certificate of the FNDS is checked for this string, and it is a friendly net only if there is an agreement.

Issuer Certificate's Fingerprint

In order to provide the maximum security against counterfeiting, the fingerprint of the Issuer Certificate has to be verified. It must match the hash value entered here.

Check for friendly networks periodically

This type of peridiodic testing can not be used if the recognition of the friendly network is done via DHCP!

The periodical testing should then be enabled when a change to the condition of the network adapter has not occurred e.g. on taking out the LAN cable. This can be the consequence of using the client in a virtual environment.

In that case this function that is checked in pre-set intervals, checks whether the client is still in a friendly network. As soon as the friendly network is no longer available the connection will be cut a new friendly network will be sought using the normal mechanisms.

An interval in seconds can be defined for the periodic check. The maximum value of 3600 seconds is preset. The check is performed regardless of when the connection is established or a media change takes place.

With a connection build-up or medium switch it is standard always to check whether a friendly network is available. (During this check the red bar symbol is temporarily on display on the monitor).

Options

Optionally, certain functions of a the Secure Client already located in a friendly network, can be grayed out.

Connection set-up not permitted in detected friendly network

If this option is switched on, an additional VPN tunnel cannot be established if the Secure Client is already in a known network. Both the button for connection set up and the menu item in the Secure Client Monitor are deactivated. An existing VPN connection that may have been established by a different application can be disconnected.

Mask out Logon Options in detected friendly network

If the Secure Client is already in a friendly network, the logon options for domain logon can be hidden.

Timeout for FriendlyNet detection before Windows logon

The timeframe for automatic Friendly Net Detection can be entered independently from the timeout value. The value for the network search time must be at least 30 seconds. (Default is 60 seconds).

Actions

When the client detects a change from known to unknown networks (or the reverse) or the Home Zone [200] is activated, an action can be triggered. For example, an external program or batch file could be started that changes the Windows system proxy settings.

Applications / Batch Files

Click "Add" and then select either an application or a batch file (*.com, *.exe, *.bat).

The application can be manually input with the path name, or the path will be input with the help of an environment variable.

The following variables are supported:

• **NCP variables: %SYSTEMROOT%, %INSTALLDIR%, %PROGDIR%**

• **Windows environment variables: z.B.: NcpClntInstallPath, ProgramData**

The path of the application to be resolved can contain blanks, but in this case must be set in speech marks.

Eg: "%INSTALLDIR%Ncp Client Cmd.exe" /connect

If the environment variables on entry were given by the user or by the central administration (on the drafting of the configuration files ncpphone.cfg and ncpphone.cnf), then the environment variables will be converted into the corresponding local paths as soon as they have been saved and read into the client monitor.

Start option

The application / batch file can be started when the Secure Client has detected a friendly network or the network adapter is located in a friendly network.

The selected application / batch file could also be started when the Client can not detect a friendly network or the network adapter is not located in a friendly network.

Wait until the application is finished (wait)

The applications and batch files will be started, dependent on the start option, in the sequence in which they are listed in the actions overview table, i.e. the sequence of those for a friendly network or for an unfriendly/unknown network.

The execution of applications (*.com and *.exe) in the corresponding sequence can be halted with the Wait function, i.e. the next application will only be started when the action marked with the Wait function has been deliberately terminated by the user.

Please note the following when creating batch files.

The Wait function will only work with a batch file when that batch file has an error, e.g. halts prematurely, that makes it unable to correctly execute all the commands in the batch file. If, in this case, the Wait function is set, then the batch file must first be manually terminated before the subsequent application/batch file in the list will be started.

In such a case, the user must be informed by suitable feedback from the batch file.

Applications / Batch Files Overview Table

Initially, actions are listed in the overview table in the sequence in which they were created. Use the green arrows at the RH border to alter the sequence of the actions.

In order to improve the overview, group all the actions together, one after the other, according to whether they will be started on detection of friendly or unknown (unfriendly) networks.

Options [Firewall]

Use settings in the "General 71" folder to activate the Firewall even when the Secure Client has not been started.

Use settings in the "Commands 73" tab to define password and time span that will then be used to temporarily open the firewall from the command line; similarly, configuration settings for hotspot logon can be entered.

General

Keep Firewall active after Client has been terminated

The firewall can also be held active, even when the client is stopped, provided this function is selected. In this state each incoming and outgoing communication is suppressed, so that no data traffic at all is possible, as long as the client is deactivated.

If this function is not set and the client is stopped, then the firewall will also be deactivated.

Enable Stateful Boot Option

If the firewall is set active even if the client is stopped, you can use this function to switch on stateful inspection. In this way the communication from the computer to another network is possible.

This setting is active after restarting the service (reboot).

> **Note:** If you import a configuration file during client installation, you must reboot the system. This reboot happens independently of the reboot that is required after installation. If this reboot does not occur, your setting is shown as active but is not yet effective at the driver level.

UDP Pre-filtering

In the default setting, when you start the client (independent of the firewall) UDP packets are filtered out so that a connection to the client computer from the outside is not possible. If you start an application with server function on the client computer, which is based on UDP data transfer (e. g. terminal applications or NTP), then this default setting can have a disturbing effect on data communication. Consequently this default setting can be switched off, or it can be limited to UDP packets of unknown networks.

always: Default setting. In this setting, no UDP packets reach the client PC when the client is running.

only for unknown networks: In this setting, UPD filtering discards all packets from unknown networks.

off: If the filter is switched off, all UDP packets reach the client PC. This setting should only be used if problems occur with an application.

Protect VMware guest operating systems

A VMware guest system can be protected by a client installed in the host system, if the firewall is activated. This means that the firewall of the Client has to be active. The guest system cannot then receive incoming connections.

VMware supports various networking modes for the guest system: Bridged, NAT and Host Only.

Host Only Mode

If Host Only Mode is used then, independent of the firewall, the guest can always communicate bidirectionally with the host system.

Bridged Mode

When in bridged mode and with the option "Protect VMware guest operating systems" enabled, the guest system is completely sealed off. In this mode, there is no possibility of setting up a connection to or from the Internet and even DHCP requests are blocked.

Nat Mode

When in NAT mode and with the option "Protect VMware guest operating systems" enabled, the configurable firewall rules apply to outgoing connections. It is not possible, however, to set-up an incoming connection.

To activate this, enable the "Protect VMware guest operating systems" option in the monitor "Firewall" menu under the "Options" tab; when enabled, bidirectional communication between guest system and host system will still be possible.

Reject outgoing traffic

This parameter defines the subsequent handling of outgoing packets blocked by an existing firewall rule:

If "Reject outgoing traffic" is ENABLED (box ticked) (default setting), outgoing packets that are blocked due to currently active firewall rules will be acknowledged to the sending application with "Reject" (ICMP destination unreachable). Applications are usually already programmed to handle "ICMP destination unreachable" as an acceptable network error and handle it accordingly.

If "Reject outgoing traffic" is DISABLED, outgoing packets that are blocked due to currently active firewall rules will be dropped without acknowledgement to the sending application. As the outgoing packet is simply dropped without any acknowledgement, the application responsible must wait for network timeouts to expire before taking any exceptional action.

Activating the Home Zone

To use the Home Zone Feature [200] at least one adapter (LAN or Wi-Fi) must be available for connecting to the private network.

Temporarily enable Home Zone

If the Home Zone is only temporarily available, this switch can be set. This will cause the home zone settings in the firewall to be reset when the home zone is no longer actively used.

This is the case, for example

- when services are stopped and started
- if a network change from LAN to WLAN or vice versa takes place (under the setting WLAN off if LAN active)
- if the network adapter is deactivated / activated
- when the LAN cable is unplugged or inserted
- when the system is restarted

Commands [Firewall]

Allow to disable the firewall temporarily for a given amount of time using the command "RWSCMD / FirewallOff".

If it should be possible to temporarily open the Firewall via the command line, this function has to be activated.

In this case, entering a password is optional. If a password has been entered here, it must be repeated in the command line.

The command is:

rwscmd /firewalloff [Password] [Timeout]

A timeout can be set in the command line in seconds (whole-numbers).

The Firewall is enabled again if either the timeout expires or the command "rwscmd /firewallon" is entered.

rwscmd /firewallon

In this case, entering a password is optional. If a password has been entered here, it must be repeated in the command line.

Input of the "Max. Timeouts" is optional. The value entered here is for limiting the timeout, which has to be set in the command line.

Additional ports are opened if they are entered in this field, apart from the default ports 80 and 443 which are automatically opened for hotspot logon. Separate each port from the next by a comma. Accordingly further port ranges are opened if they are entered in this field (e.g. 50100-50200). Separate each multiple port range from the next by a comma.

Logging

Dependent on settings, the activities of the Firewall are written into a log file. The default location of the output directory for logfiles is in the installation directory under [installdir]\log.

The log files for the Firewall are written in pure text format and are named fwyymmdd.log. (yymmdd =year, month, day) They contain a description of "rejected data traffic" and/or "permitted data traffic". If neither of these options has been selected, only status information on the Firewall will be logged.

The logfiles are written at each start of the Firewall. The maximum number maintained in the log directory is defined by the number of the "days of logging".

Important: performance is negatively affected while logging is activated, as log text must be written for each individual packet.

VPN bypass

The VPN bypass function 204 allows the administrator to define applications or domains which can communicate over the Internet directly despite disabling Split Tunneling 190 on the VPN connection It is also possible to define which domains can bypass the VPN tunnel.

This function can be used to separate non-sensitive data traffic from the central infrastructure, so as not to affect performance. For example, operating systems and virus scanner updates (with a known domain), can bypass the VPN connection easily, or certain cloud services direct can per permitted direct access to applications via the Internet.

Configuration

• Firstly the applications or domains which need to bypass the VPN tunnel are defined in this configuration menu. Additionally it can be defined whether the VPN bypass function should apply to TCP or UDP traffic.

• The created bypass list of applications or domains for a VPN bypass will be selected for further configuration in the profile settings of VPN Bypass 191. Therefor you define a special VPN bypass to be used by the currently selected VPN profile.

Quality of Service

To configure Quality of Service, also note the detailed [configuration description](#) 210 of this feature.

When opened for the first time, the list of configurations is still empty (see figure below).
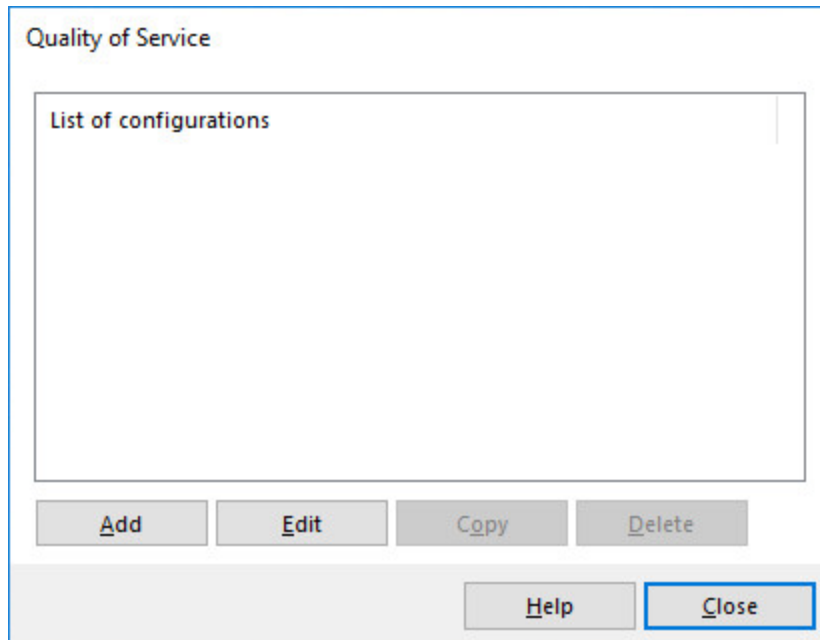
Click "Add" to open the first configuration dialog (see figure below).

Type in a name for your configuration (in the picture above "My-QoS-Configuration"). Then enter the maximum available network bandwidth in MBit/s for this group. (The total available bandwidth can be taken from the contract with the network service provider or determined with a speed test. See "Connection / Connection info" in the main menu). A maximum of 100 MBit/s can be entered. The upstream default value for VDSL is 10Mbit/s.

Group Configuration

It is possible to configure different groups (see figure below) by clicking "Add".

Click "Add" and type in a name for the new group (fig. below "Video / Skype"). Here you can also determine the minimmum bandwidth for this group.

By clicking "Ok" the new group will be added to the configuration (fig. below). Further groups are created in the same way.

Note that when configuring multiple groups, the network bandwidth must not be exceeded. Otherwise the configuration can not be saved.

Filter Configuration

In the configuration of a group it is possible to define filters. Open a group by double clicking or using "Edit". With "Add" you can create a new filter and define what kind of type it should be - application or directory.
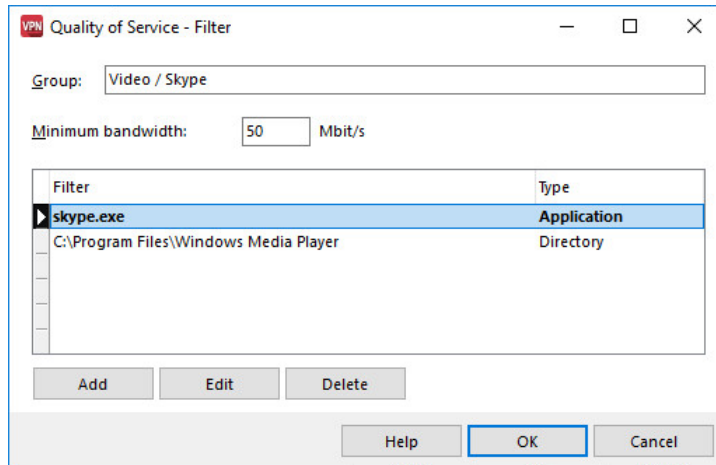
By clicking "Add" a new window opens with the option to choose the type for new filter.

Application: With this type you select the application for which the entered bandwidth is ensured. If you know the name of the application (eg skype.exe), you can enter it directly in the field (see picture below).

Directory: This type selects all .exe files that are in the specified directory.
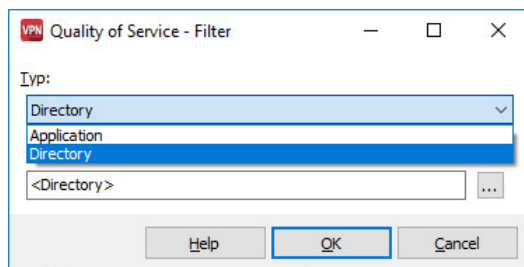
Depending on the selection of the type, a field for the corresponding entry is also offered.

After the filters have been added, they are displayed as in the figure above.

Note that every filter has not its own minimum bandwidth. The definied minimum bandwidth refers to the group. If several filters are active simultaneously, the bandwidth will be shared with all filters in the group. To increase the bandwidth of a filter, the filter should be included in a separate group.

How to use Quality of Service in a VPN Profile

To use a Quality of Service configuration it must be assigned to a profile. These configurations can be assigned to profiles in the menu under "Configuration / Profiles". Choose via double click the profile which should receive the configuration.

Under "Extended Configuration \ Connection 157" you can add one of your configurations to "Quality of Service".
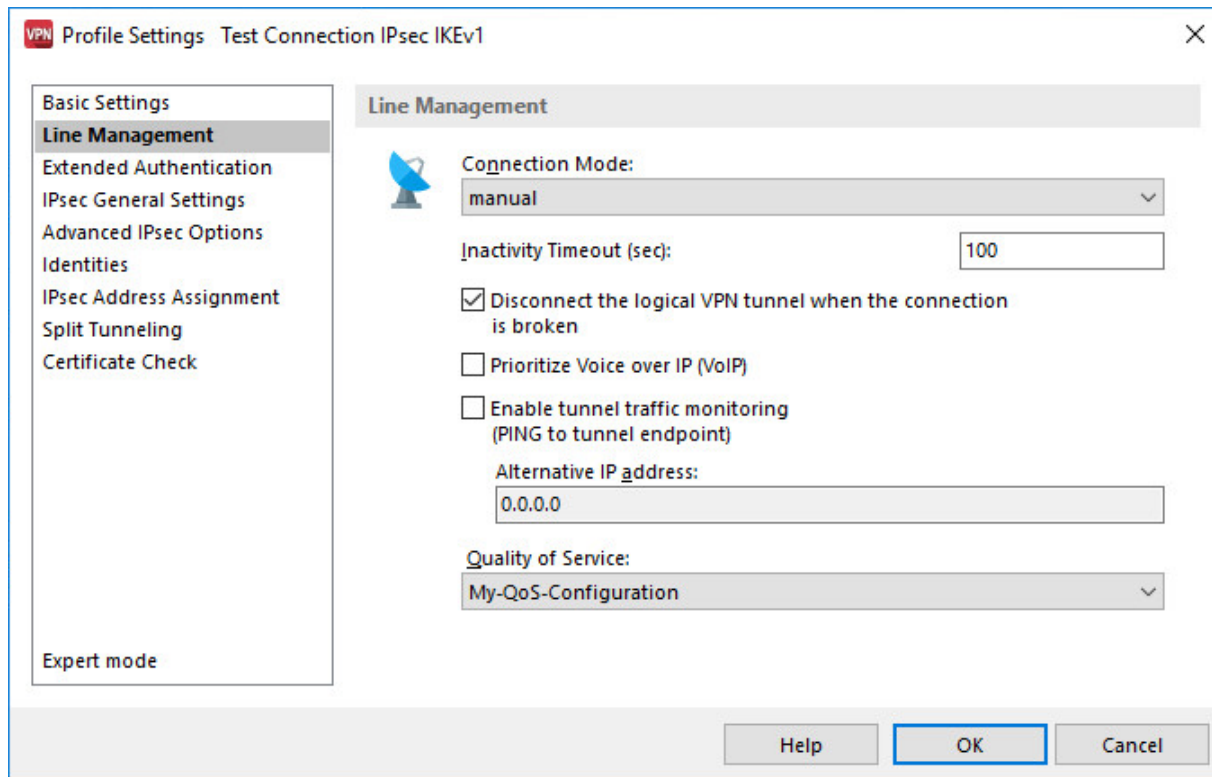
Wi-Fi Management

Enable Wi-Fi Management

When Wi-Fi management of the client is enabled, the automatic Wi-Fi detection and easy Wi-Fi hotspot logon can be used.

To create WLAN profiles with the management tool, settings can be made in the following configuration windows:

Wi-Fi Management

If Activate WLAN Management is enabled and the Options Enable Hotspot/Wi-Fi Detection is enabled and no internet connection is available, a panel will be shown for each existing Wi-Fi network in the client interface with a link and a button.

Click the link or button to establish a hotspot connection (of the current VPN profile) automatically if a Wi-Fi profile in the list of the Wi-Fi Manager is set to connect automatically.

If no Wi-Fi profile is selected with automatic connection in the Wi-Fi Manager list, the Wi-Fi Manager list will open. When the Connect button next to the selected Wi-Fi profile is clicked, the hotspot connection will be established. At the same time the automatic connection will be enabled for the selected Wi-Fi profile which will remain connected until the VPN connection is disconnected manually.

After hotspot authentication the VPN connection is established. The user may need to enter authentication details for the VPN.

If the hotspot logon or an encrypted connection to the access point is successful and an internet connection is available, the VPN will connect automatically using the current VPN profile without the users intervention.

Note that the automatic hotspot logon as described above cannot be used if the media type Mobile network is enabled for automatic media detection and the last VPN connection was established via a mobile network (or if the client is in seamless roaming mode).

Hotspot Connection without Wi-Fi Automatism

If the user does not use the link provided by the wizard in the client GUI and instead uses the clients Wi-Fi manager directly, a connection to the wireless network including hotspot logon can be established without starting the VPN connection.

External Wi-Fi Manager

If the Wi-Fi manager of the client is not enabled as described above, an application from another manufacturer (e.g. Microsoft wireless network configuration) must be used.

In this case the Hotspot Logon menu item will be displayed under the Connection menu in the client. When clicked, this menu item will prompt the user for an encryption key before a separate browser window is opened for entering the login details.

Connections

In order to display the "Network Search" tab, located under the "Configuration / Wi-Fi Settings", Wi-Fi must be selected as "Medium".

If "Enable Wi-Fi Management" is set (tick in checkbox), the Wi-Fi card management tool or the Microsoft Wi-Fi management tool is deactivated and all management of the card is taken over by the Wi-Fi management tool. (Normally, enabling one Wi-Fi management tool automatically disables all other tools installed.)

Adapter

As soon as one more adapter is installed it is displayed. If several adapters are available, select one.

Wi-Fi access points

After a few seconds of automatic scanning, all Wi-Fi networks available are displayed with data like SSID, signal strength, encryption and profile.

If there is no profile for an SSID, yet, like after first installation of the client, a profile can be set up via double click on the SSID in two steps only with the help of a wizard (see below Wi-Fi profile).

SSID / Signal / Encryption / Profiles

The name for the SSID (Standard Security) is set by the network provider and displayed below the GUI of the monitor as well as in the tray icon. The SSID is automatically transferred to a Wi-Fi profile for this adapter after double clicking on it if no profile as been set up for this profile, yet.

The signal strength of the Wi-Fi network is displayed graphically.

The respective encryption (WEP, WPA, WPA2, WPA3) are displayed behind the encryption symbol.

If there is already a profile available, this is displayed with a star. If this profile is also configured for Wi-Fi automatism there is a star with "Auto" written on it.

Wi-Fi profile

Double click on the SSID for automated configuration of a Wi-Fi profile. The first step is to enter the key (which you have received from the access point administration).

The second window of the wizard offers you to add this Wi-Fi profile to the Wi-Fi automatism (see below) which can be configured later on, too. (Independent of assigning this profile to Wi-Fi automatism, after clicking on "Finish" the client immediately tries to set up a connection to the access point.)

After the connection to the access point has been established, a click on disconnect in the tray icon (in the list of SSIDs) terminates this connection.

Wi-Fi automatism

If several profiles have been configured with Wi-Fi automatism and this feature is activated, first the system tries to establish a connection with the last profile used. If the SSID does not match and no connection to the access point can be set up with this profile, all profiles with Wi-Fi automatism are used for connection set up in the order of configuration until a profile with matching SSID is detected and used. (Please also refer to the section Profiles.)

Notify user for available open networks

If this function is used Wi-Fi networks without encryption are displayed. These can be used for hotspot logon. This is displayed with an icon next to the tray icon.

Profiles [Wi-Fi]

All configured profiles are displayed in a list. All profiles with Wi-Fi automatism are marked with a check mark. The selected profile can be moved up or down with the green arrow buttons. The Wi-Fi automatism feature always works through the list from top to bottom until it reaches a profile with which a connection to an access point can be established. If a profile, which has not yet been configured for Wi-Fi automatism, is to be configured for Wi-Fi automatism, it has to be opened with double clicking the edit button and "Auto-Connect" has been checked.

A new profile is set up by clicking the "Add" button. Alternatively a Wi-Fi network can be either double clicked or clicked on with the right mouse key in the Wi-Fi settings window.

The profiles can also be edited or deleted via the buttons.

General Profile Settings

Name

The name can be assigned freely and after set up of a new profile via double clicking on the scanned network, it is identical to the SSID of this network.

SSID

The SSID is entered automatically as soon as it is scanned, while for hidden networks it has to be entered manually.

Power mode

If the WLAN adapter permits it the energy mode can be selected.

Auto-Connect

If the feature "Auto-Connect" is activated for this profile it is placed in the profile list of Wi-Fi automatism and selected if needed.

Hidden SSID

Hidden networks are displayed without SSID, i.e. they cannot be selected via its SSID for a connection to the access point.

If your Wi-Fi network is configured as hidden network, activate this feature and enter a name for the profile manually configured. You can use the name later on as selection criterion in the tab "Search Networks".

Disconnect if VPN gets disconnected

Security in a hotspot environment is increased by setting the option.

Metered Connections

If the media type of connection of the VPN tunnel is changed from LAN to a mobile connection resulting in connection costs, this can be communicated to the server (prerequisite SES 11.x). For this purpose, the "metered connection" setting must be activated in the Wi-Fi profile under "Wi-Fi Profiles / General". (Default: disabled)

For better management of metered connections, the client receives an IP address from the server from a pool for clients using a mobile connection during tunnel setup.

This is also the case if the client does not directly establish the mobile connection, but is connected via Wi-Fi to an LTE router.

If the setting for "Metered Connection" is changed, an existing WLAN connection to an access point must be disconnected and re-established, otherwise the configuration change will not become active.

Encryption [Wi-Fi profile]

The encryption mechanism must be specified by the Access Point (Wi-Fi router) and communicated by the administrator.

The option "EAP" can be added under for WPA encryption. The prerequisite in this case is that a certificate must have been configured. Regardless of the EAP configuration, EAP with certificate is always used here.

Configuration of a Wi-Fi profile with 802.1x authentication

Note

Securing a Wi-Fi connection is possible with the help of 802.1x authentication. Refer to the Microsoft documentation for the requirements and setup.

Note that the certificates required for authentication must be stored in the certificate store before configuring the Wi-Fi profile in Windows. The issuer certificate of the remote peer (such as the Wi-Fi access point) should be stored with the "Trusted Root Certification Authorities" in the computer certificate store. The certificate with which the computer authenticates itself can be a user certificate or a computer certificate, as desired, and is stored under "My certificates" in the user or computer certificate store.

The certificate configuration of the client is possible via the NCP Wi-Fi Manager.

To configure an 802.1x authentication in a Wi-Fi profile, proceed as follows:

1. In the client interface, click *Configuration* and select *Wi-Fi*.

2. Create a new Wi-Fi profile via *Add* in the *Profiles* tab or open an existing profile.

3. Select the *Encryption* tab. Under Encryption, specify a WPA encryption (WPA3, WPA2 or WPA) for this profile and under *Key Management*, specify the key *EAP*.

4. Use the *certificate selection* to choose your desired certificate. You can also select the smartcard or certificate properties here.

5. Click *OK* to accept the configurations.

IP Addresses [Wi-Fi profile]

Configure the IP address of the Wi-Fi card in this window.

The settings made here are only effective if the Wi-Fi configuration has been activated as described above. In this case the configuration entered here will be transferred into the Microsoft configuration of the network connections. (See: Network connections / Properties of Internet protocol (TCP/IP)).

Authentication [WLAN profile]

The access data for the hot spot must be entered in this window. These user details are only used for this Wi-Fi profile.

Authentication can be executed by entering user ID and password, or via script. The script automates the logon to the hot spot operator.

Please note that there are charges associated with the connection via a hotspot operator. You must agree to the terms and conditions of the hotspot operator in order to set up the connection.

No Authentication at the Hot Spot

If the connection to the companys own access point in the local area radio network is to be established without a hotspot, select no hotspot authentication.

You should choose no hot spot authentication if the hotspot operator does not support script-controlled authentication.

In this case, the providers login screen for entering user ID and password appears in the browser when the connection is being established. Access to the hotspot and the hotspot operators billing procedure uses this identifier. (See below hot spot Logon).

Hot Spot Authentication

Please note that, for authentication at the hotspot, you need to agree to the hotspot operators business terms before the profile can be saved and the connection established.

Authentication via Script

The script automates the login with the hotspot operator, since the logging in is done, controlled by a script, in the background, without using a browser.

Other

You select other if you are using a different hotspot, not specifically listed, for the script-controlled login. (T-Mobile, e.g., is specifically named.)

Script File Name

Script file names can be displayed for selection with other hotspot operators. You select the appropriate script for your hotspot from this list*.

* (Scripts are created on request. A script is imported into the installation directory under .)

User ID / Password

The user ID and password are entered in line with the providers guidelines.

T-Mobile

The T-Mobile hot spot can be selected for logging in using WISPr technology. A script name does not necessarily need to be selected. The corresponding script is automatically loaded in the background.

User ID / Password

Now you just need to enter the user ID and password in line with the providers guidelines.

WISPr Login

The Secure Client supports the new hot spot login technology via the WISPr (Wireless Internet Service Provider roaming) protocol. This ensures compatibility with T-Mobile hotspots in Germany, Austria, the Netherlands, the Czech Republic and Great Britain, as well as in Lufthansa lounges in certain international airports.

The WISPr login is done, script-controlled, without a browser. The script is automatically loaded in the background for the specifically named hot spot operators (e.g. T-Mobile).

You create a Wi-Fi profile with default settings. I.e. the encryption remains switched off and the IP addresses are assigned automatically.

In the configuration field for authentication, you select a specifically named hotspot operator from the list. There you will find T-Mobile (see above) and others. We are constantly updating this list of WISPr-capable hotspot operators.

With "Others", not listed here, the script-controlled, browserless login is done in a different way. (See Script file name, above).

Options [Wi-Fi profile]

Disable Wi-Fi when LAN cable is connected

With help of the function mobile teleworkers are saved some manual switching. As soon as a teleworker, who is connected via WLAN with the company network, plugs the LAN cable into his Notebook inhouse, the WLAN adapter is deactivated and the LAN connection into the company network is used.

That happens independent of whether the WLAN manager of the client or that of an unknown producer is used. When the LAN cable is unplugged, the WLAN adapter is again activated.

Enable Hotspot/Wi-Fi Detection

When this option is enabled and the mobile client is not currently connected to the internet and a wireless network is available this will be detected and the following message will be shown in the monitor on the Wi-Fi panel.

"Wireless networks are available. Click here to connect."

Click to connect and start the Wi-Fi Manager (see Wi-Fi Management).

The Wi-FI profile which is selected for the connection will be saved for automatic connection in the Wi-Fi Manager list (this also applies to previously unknown wireless networks) and a connection is established to the access point.

If the wireless network requires additional authentication, a browser window is displayed for entering the login details.

(For encrypted wireless networks, the key will also be required if this network has not already been saved in the Wi-Fi profile.)

Once internet access is available after logging on to the hotspot and / or an encrypted connection to the access point has been made, the VPN connection is established automatically.

Statistics

The statistics window for the Wi-Fi settings shows the status of the connection to the Access Point in plain text.

Certificates [Configuration]

Here you determine whether you want to use certificates for authentication of the client and where you want to store the user certificates.

Further configuration fields define the PIN policy and set the time interval within which the certificate expires or a certificate renewal must be requested

Settings for the following parameters can be made:

User Certificate 95
PIN Policy 99
Certificate Renewal 99
Hardware Certificate 99

Name and "Standard Certificate Configuration"

For each Secure Client a large number of certificate configurations can be created, with a unique name for each.

The certificate configuration of a client older than version 9.1 will in case of an update to this version automatically be converted to the default PKI configuration. The default PKI configuration will also be set up after a first installation of version 9.1 if a test connection with certificate is established.

For each profile you can select one of the stored certificate configurations. In this way, you get the option of various ways for authentication with different certificates against different VPN gateways. E.g. authentication with soft certificate against gateway 1 and authentication with certificate from token against gateway 2.

In the configuration field Identities select the certificate configuration to be used for extended authentication.

User Certificate [Configuration]
Certificate

Define here whether or not you want to use the certificate and hence use "Extended Authentication", and where the certificate is stored.

none:

The default value is "None", meaning that certificates will not be used.

from PKCS#12 file:

In order to use a soft certificate select "from PKCS#12 File" and then select the directory (path) where the PKCS#12 file is stored for access purposes. Normally you will receive this file (encrypted) from your network administrator or your CA (Certification Authority).

from smartcard:

In order to use smartcard based certificates select "from smartcard" and then select the smartcard reader from the list of supported smartcard readers. (See also: Enter PIN)

PKCS#11 module:

Select "PKCS#11-Module" from the list in conjunction with "Extended Authentication" in order for the respective certificate to be read from a smartcard in a smartcard reader or from a token.

CSP User Certificate Store:

If you select the "CSP user certificate store" from the listbox, the certificate from the CSP user certificate store is used for extended authentication. Please enter the certificate's "Subject CN" (common name) and "Issuer CN" in the respective fields.

The client supports the input of environment variables of the system at this point to make a more precise certificate selection.

Note the following about variables:

- Multiple variables can be inserted like this: %VARIABLE% / %VARIABLE%.

- If a variable cannot be resolved, it will not be replaced by any value.

- The variables will be resolved immediately after closing the configuration window.

- If a single percent sign is prefixed, all following variables are ignored.

- Double percent signs are not supported like a single percent sign.

- If a new configuration is imported into the client, these entries are replaced and entered here when a new configuration is read in.

The subject or issuer name is the complete X.500 name, individual elements are separated by commas. Here are some examples of X.500 names in certificates:

```
CN=NCP engineering GmbH, OU=Digital ID Class 3 - Microsoft Software Validation v2,
O=NCP engineering GmbH, L= Nuernberg, S=Bavaria, C=DE

CN=VeriSign Class 3 Code Signing 2009-2 CA, OU=Terms of use https:\
\verisign.com\rpa (c)09, OU=VeriSign Trust Network, O="VeriSign,Inc.",

C=US CN=NCP Demo CA 1, O=NCP, S=Bayern, C=DE, S=Bayern, L=Nuernberg, O=NCP,
OU=ou3, OU=ou2, OU=ou1, E=123456.de, SN=F, G=T, CN=TF
```

Note

The individual elements are not sorted, but in the order in which they appear in the certificate.

Smartcard Reader:

In order to use the smartcard's certificate with your card reader, select the respective smartcard reader from the list (see also PIN Entry).

The Client Software automatically supports all PC/SC conform smartcard readers. The Client Software automatically recognizes the smartcard reader each time the PC is re-booted. Thereafter the installed smartcard reader can be selected and used as required.

Port:

If the Installation has been executed correctly, the card reader will automatically be assigned a port. Should problems arise, COM Ports 1-4 can be manually assigned.

Certificate Selection:

1. Certificate ... 4.:

(default = 1) Up to 4 different certificates, located on the smartcard, can be selected from the list. The number of certificates on the smartcard depends on the Registration Authority that has issued the smartcard.

The following types are supported:

Telesec TCOS 3.0 Signature Card 2.0

Atos 5.0 and 5.3 smartcards

Other than those mentioned above can only be used via the CSP or PKCS11 interface.

For further information please contact your system administrator.

PKCS#12 File Name:

If you are using the PKCS#12 format, then you will receive a file from your system administrator that must be copied to your PC's hard disk. In this case enter the path and filename of the PKCS#12 file or alternatively after clicking the selection button [...] select the file.

Important: The path for the filename can be abbreviated by entering the variable %CertDir% (the installation directory of the user certificates). E.g.:

%CertDir%/Test.p12

CSP User Certificate Store:

If you select the "CSP user certificate store" from the listbox, the certificate from the CSP user certificate store is used for extended authentication. Please enter the certificates "Subject CN" and "Issuer CN" in the respective fields.

Since this function is only available after the users logon to the windows system, it cannot be used for domain logon via VPN (see Hardware Certificate)!

Extended Key Usage:

You can preconfigure the default certificate for a user or computer for authentication oer encryption purposes.

PIN Request at each Connection

Default: If this function is not used, the PIN request is displayed only for the first connect of the VPN/PKI Client.

If this function is activated, the PIN will be requested at each connect.

Certificate Selection

PC-Sharing (Using multiple Soft Certificates on one Client PC)

If you want to set up PC-sharing for multiple users, who use a separate certificate each, then you configure this under "User Certificate".

Under the tab "User Certificate" you check "Enable Certificate Selection" and select a "Certificate Path". If this path has been created previously, then you can select this path via the select button. (e.g. %CertDir%). The various user certificates must then be created under this path.

If these settings are saved with "OK", then the certificate list appears under the graphic field of the monitor, with the list of all user certificates saved under the certificate path (for instance user1 to user4).

If the user has selected his soft certificate (user2 for instance) and has established a connection to the central VPN gateway, then he has to enter his PIN first. Then the connection to the destination system will be established.

If the user leaves the workstation, then he should use the "Logout" button. This completely dismantles the connection and resets the PIN (this also occurs if another certificate is selected during an existing connection). If there is no logout, then non-authorized users can obtain access to the VPN Gateway via the existing connection.

A subsequent user proceeds in precisely the same manner. First he selects his certificate, then clicks on the "Connect" button and enters his PIN. Only then can the connection be established correctly. If the user leaves the workstation, then he clicks on the "Logout" button.

Activate Certificate Selection

This function is used only for PC-sharing, when multiple users of the PC work with different soft certificates.

Certificate Path

Different soft certificates of multiple users on this PC can be stored under this path.

PIN Policy

Minimum number of characters

Default is a 6-digit PIN. An 8-digit PIN is recommended for security reasons.

Further Policies

It is recommended to implement all PIN policies, other than the one specifying that only numbers may be contained. Additionally, the PIN should not begin with a number.

The specified policies are displayed when the PIN is changed, and the policies that are only fulfilled at entry are highlighted in green (see: Change PIN).

Certificate Renewal

In this configuration field specify whether a message is to be displayed that warns of the expiration of validity, and also specify how many days prior to the certificate validity expiration this message should be displayed. After the prior date and time are reached, a message is displayed each time the certificate is used, indicating the expiration date of the certificate.

Hardware Certificate

In order for the additional authentication to be used with a hardware certificate, the "Hardware certificate CN" option must be activated under Link profiles at the gateway.

With a hardware certificate, the computer authenticates itself to the gateway. If it is used in addition to a user certificate, it can be ensured that the user always dials in from the same computer.

Link Options [Configuration]

Under "Link Options" configure the budget manager and those applications or batch files which should be started, dependent on the state of a VPN connection, by the Client Monitor.

See also the topics:

Budget Manager [Configuration]
Budget Manager Functions

The budget manager is a component of the Secure Client "Link Options" and serves predominately for voluntary self-monitoring. It measures and monitors the data volume estimation during a certain time span or the time run out online within this time span (e.g. within a month), provided the connection has been built via a media type supported by its own dialer. If no parameter locks are created by the administrator in the client software, the user can set the budget limits himself.

Should a limit be exceeded and a connection establishment is no longer possible, the user must contact his administrator, provided parameter blocks are set. The parameter blocks must be undone; only afterwards can the user conduct a new configuration.

See following topics:

Settings [Budget Manager]

Budget Limitation according to Volume or Time online

The corresponding settings, whether data volume or time online that should be measured during a month or other determined time period, can be done via the monitor menu "Configuration / Link Options".

For all communication media supported by its own dialer, each type of calculation can be determined separately, whether the (monthly) connection volume or the time of connection are measured. So for example, a maximum connection time per month for Wi-Fi and a maximum connection volume per month for Mobile Network can be specified.

Smaller Budgets for Mobile Computing

If a limited budget is available for a limited time period, for example for the time of a hotel stay, the starting time can be set manually. For this, the statistic is opened via the monitor menu "Connection" and in order to reset the statistics press the reset button. With this, the starting time is determined from which the specified budget is posted. (Pressing the reset button again starts the connection control again with the same specification and deletes the previous connection records.)

Actions [Budget Manager]

Budget Statistics and Automated Warnings

The user obtains an overview of his (monthly) budget in the statistics regarding connection control. The statistic shows, with the current date, how much of the maximum exhausted budget in hours or bytes already have been used since the first of the current month or since the start of monitoring. Here you can also see the limits that can be set in order to trigger certain actions.

The actions are individually determined like the connection control for each medium. This means a warning can be issued after a certain percentage of determined connection volume or the maximum connection time that alerts the user that the budget is soon exhausted. Or, after the budget is exhausted, no further connection is permissible for this month.

If the budget display in the statistic is clearly more rapid than the balance display for the calendar, the assigned budget is not sufficient. The budget display is coloured yellow after reaching the warning area, red after reaching the maximum value. If establishment of the connection is no longer permissible after exceeding the maximum value, the corresponding report appears on the client monitor.

Mobile Network [Budget Manager]

Avoid costly Roaming

For the media type Mobile Network, the connection control is activated separately for inland (home) and roaming connections. Unnecessary roaming with Mobile Network connections, e.g. in border areas, can largely be excluded through targeted security inquiries. In this way, lists of permissible inland network operations and permissible roaming network operators can be created that conveniantly permit the selection of the most favourable and the general exclusion of undesirable providers.

Inland Network Operator and Roaming Network Operator

Like the connection control, which is activated separately for inland connections and roaming connections, separated lists for permissible inland network operator and roaming operators are conducted. Via these lists that are conducted in the settings "General", the provider selection is automated. Each provider, that the user has entered via the automated network operator administration or manually in one of the lists under "inland" or "roaming", is used for connection establishment as soon as the system recognizes it. Yet unknown providers are handled according to the setting for impermissible network operators.

Automatic Provider Management

If automatic provider management is activated, the user is asked for each new provider not yet known to the system into which new providers' list this provider should be recorded: In the list of inland network operators, of the roaming network operators or denied impermissible network operators. The list of network operators to be denied can be handled under "Upgrading" at any time, for example in order to delete a provider and to record it in another list.

If automatic provider management is not used, a provider, the system does not yet recognize, is handled as an impermissible network operator and connection establishment is made via this provider according to the options for impermissible network operator specified under the settings "General".

Wi-Fi Access Points [Budget Manager]

Call Control Management for Individual Wi-Fi Profiles

For each Wi-Fi profile that has been configured on the monitor menu "Configuration", a separate call control manager can be set. Additionally, the SSID is transferred from the prevailing Wi-Fi profile in the call control management for the Wi-Fi network. The call control management can be activated individually via the "Settings" or for several in the overview under "Wi-Fi".

External Applications

Functions

After you have selected the function Start External Applications or Batch Files you can select an application or batch file with the insert button, which can be loaded with a start option:

• execute before a connection has been established (precon)
• execute after a connection has been established (postcon)
• execute after a connection has been disconnected (discon)
If you want to start the default browser after connection set up, then activate this function and enter the web site of the browser.

Additionally these applications to be carried out can be bound to a specific profile. That profile can be selected from the list of profile settings already available, after you have clicked on the insert or edit button.

Watch out that no commas appear in the name of the profile selected! The function fails and the external application will not be started, if there are commas in the profile name!

Deny the start of the "(dis)connect.bat"

This function should always be activated

• if execution of the cited batch files with administrator rights (system rights) is not necessarily required for a desired application. (Please refer to the the description in the "Services" appendix in the manual).

The applications (batch files) for which user rights are adequate, can be started in the monitor menu "External applications..." (see above).

Options [Mobile Connection]

Disable mobile network when LAN cable is connected

With help of the function mobile teleworkers are saved some manual switching. As soon as a teleworker, who is connected via mobile device with the company network, plugs the LAN cable into his notebook inhouse, the LTE/UMTS device is deactivated and the LAN connection into the company network is used.

When the LAN cable is unplugged, the LTE/UMTS device is again activated.

Disable mobile network when Wi-Fi connection is established

As soon as a teleworker who is connected to the company network via mobile phone can use a connection to the company network via WLAN, the LTE / UMTS adapter is deactivated.

If the WLAN connection is lost, the connection via the LTE / UMTS adapter is activated again instead.

Logon Options

To enable a VPN connection to a windows domain before the user logs on, the option Display connection dialog before Windows logon 107 must be enabled from the Logon 107 tab under the "Logon Options" item in the "Configuration" menu.

When this option is enabled further configuration options will be activated under External Applications 109 and Options 110 tabs.

See also the feature description for the Credential Provider 207.

Logon [Logon Options]

Because the connection set up to the gateway occurs prior to the Windows logon, the logon to the remote domain is already encrypted and the firewall is activated.

Display connection dialog before Windows logon

The dialogs of the logon option (Credential Provider) can be hidden via the monitor menu without de-installing the logon option. Thus concatenations of the logon option that may possibly be necessary for the respective work environment remain intact.

If the logon dialog does not appear, the connection to the domain server cannot be set up via the logon option. In other words you must have the "Display connection dialog before Windows logon" so that in the boot phase the connection to the VPN gateway can already be set up. For this connection set up you must enter access data for the network dial-in, or PIN and SIM PIN must be entered before the Windows logon.

Windows Logon

The following Windows logon can be executed automatically or manually depending on configuration. "Execute manually" means that the user must enter his logon data manually in the Windows logon screen. Automatically means that the client software will transfer the data entered here to the Microsoft logon interface (Credential Provider) without user intervention.

The "VPN User ID" from the profile settings ("Identities") can be used for windows logon if the "Use VPN User ID for Windows Logon" option is enabled. The same applies for the "VPN Password". Enable the "Automatic Windows logon ..." option first.

If the above option(s) is enabled and the VPN authentication data (VPN User ID and VPN Password) are to be read from a field of the certificate used, this data is also automatically used for Windows logon. Alternatively authentication data can be defined for Windows logon.

Logoff [Logon Options]

The client connection to the VPN gateway or ISP can be maintained when a Windows logon is executed.

This permits a change of Windows user on the computer, without having to disconnect the VPN connection.

Disconnect after logoff

When this function is activated the connection shuts down when the system switches to hibernation or standby mode. When the system resumes from hibernation or standby mode the connection has to be reestablished.

Flush cached credentials upon resuming from hibernation / sleep

Username and password must be entered if this option is activated, as, when it is activated, the username and password will have been deleted from the cache.

NOTE: only applicable when username and password are not stored in the configuration.

External Applications [Logon Options]

Use this configuration field to start applications or batch files, depending on the Client Monitor (no Windows programs!).

Safety Instructions

Note that the application is executed within the *system context* and thus runs with elevated privileges. Executing an application prior to a login within the *user context* has to be rated as critical regarding security.

Also note that it is recommended to only use console applications and non-interactive applications, to prevent further security issues (for example, by opening the File Explorer with elevated privileges).

The external applications are added as described on the next page. The call sequence from top to bottom can be changed with the arrow buttons.

Application / Batch File

After clicking on *add*, an application or batch file can be selected. (*.com, *.exe, *.bat).

Only files located in `%BaseDataDir%\scripts` (Default: `C:\ProgramData\NCP\SecureClient\scripts\`) are available for selection.

Start Option

The application or batch file can be loaded according to its start option:

• **start before connection build-up (precon)**

• **start after connection build-up (postcon)**

• **start after client log-on (always)**

The latter start option allows the starting of applications in accordance with the EAP negotiation via the log-on option (Credential Provider) and following local registration without VPN connection.

Connection Type

In addition, the application can be started depending on the connection type of the destination system that is selected in the logon dialog. The application always starts if the connection type "All" has been selected.

Wait for domain logon to complet (postdom) means that after the initialization period, the application is started immediately.

The wait function "Wait until the application is finished" can then be relevant if a series of batch files is to be executed one after the other.

Options [Logon Options]

Lead Time

Windows requires a certain initialization time between network logon and domain logon. This preparation time for the domain logon can be activated and set here. The Windows logon will only be executed after the connection set up, after the initialization time set here has elapsed.

The default value is 45 seconds and can be changed if needed.

EAP Authentication before Profile Selection

If this parameter is activated then EAP authentication will be executed prior to the destination dialog in the credential provider and the system will ask for the necessary PIN, regardless of whether EAP will be required for subsequent dial-in. This parameter can be used, for example, if the credential provider will only be used for EAP authentication, without setting up a connection to destination system (use as a pure EAP client).

If this function is not activated, then EAP authentication will be executed after the destination selection.

If EAP with certificate is to be used, first the PIN dialog is displayed. Afterwards you can select the profile.

Automatically open dialog for connection establishment

Subsequently you can select whether a dialog should open automatically for connection establishment to a remote domain.

For the connection to the gateway it may be necessary to enter the PIN for the certificate, as well as for the SIM card and the (non-saved) password for network dial-in, before the password for the Windows logon can be entered.

If you do not activate the function in the adjacent window, then the password and PIN for the client will only be queried after the Windows logon.

Show the preselected icon of the maximized

In this case, only the credentials will be displayed.

Configuration Locks

Configuration locks can be used to make the client's interface clearer.

In addition, it can be avoided that unauthorized or accidental changes in the profile settings are made.

To set configuration locks effectively, enter "User" and "Password". The password must then be confirmed.

Please note the descriptions for the following parameter fields:

General [Configuration Locks] 111
Profiles [Configuration Locks] 111
Mobile Network 112

General [Configuration Locks]
ID for Configuration Locks
In order to effectively set the configuration locks, identification must be entered, which consists of "User ID" and "Password". The password must be confirmed thereafter.

Please note that identification is absolutely necessary to activate or cancel the configuration locks. If the identification is forgotten there is no possibility to cancel the locks!

Authorizations for Configuration
Now authorization to open menu items under the main menu item, "Configuration", can be limited for the user. As default, the user can open all menu items and edit the configurations. If the check mark is removed from the respective menu item with a mouse click, then the user can no longer open this menu item.

The editing rights for the parameters of the profiles 111 are divided into two sections.

In addition, an authorization for storing a SIM for the mobile communication card 112 can still be assigned.

Profiles [Configuration Locks]
General Rights
The general rights apply only to the profiles. If "Profiles may be created new" is specified, but "Profiles may be configured" is excluded, new profiles can be defined with the wizard, but a subsequent change of individual parameters is then no longer possible.

Visible parameter fields of the profiles
The parameter fields of the profile settings can be hidden for the user.

Please note as well that parameters of a non-visible folder cannot be configured.

Mobile Network [Configuration Locks]

Using a 3G Card the user can be allowed to store the SIM PIN.

This function is not visible in the Entry Client default setting. It becomes visible and configurable for the user when the privilege is granted to him in the configuration locks under tab "Mobile Network", i.e. "User may save SIM PIN in configuration" has been activated.

Other Options

Further configuration options are available:

Proxy for VPN Path Finder 113
EAP Options 114
FIPS Support 115

Proxy for VPN Path Finder

If the VPN Path Finder option is used under Advanced IPsec Options 180 in the configuration menu of the profiles but Internet access is only available via a proxy server, either define the proxy settings manually here or select the system settings configured under Windows.

EAP Options [Configuration]

You can specify whether EAP authentication (802.1x) will be executed on Wi-Fi interfaces, LAN interfaces, or via all network interfaces, in the "EAP Options" of the monitor menu. The setting made here applies globally for all profile entries. The authentication methods EAP-MD5 and EAP-TLS are supported.

• disabled

• for all network interfaces

• only for Wi-Fi interfaces

• only for LAN interfaces

Use of the Extended Authentication Protocol Message Digest version 5 (EAP MD5) can be specified via the main menu of the monitor under "Configuration / EAP Options". This protocol can then be used if a switch, a hub, or if an access point is used, which support 802.1x and the according Authentication Mode for the access to the Wi-Fi. You can prevent unauthorized users from getting into the LAN via the hardware interface with the Extended Authentication Protocol (EAP MD5).

You can use either User ID 185 with Password 185 (Identities 185) or your own "EAP User ID" with an "EAP Password".

For EAP-TLS (with certificate) now the EAP identity can be directly referenced from the certificate configuration. The following content of the configured certificate can be used by entering the appropriate placeholders in the EAP configuration:

Commonname: %CERT_CN%

E-mail: %CERT_EMAIL%

FIPS

Default setting: FIPS Mode deactivated

To automatically load the cryptography modules required for FIPS, enable the FIPS mode.

Note that after each state change in FIPS mode, the VPN services are restarted.

The IPsec Client incorporates cryptographic algorithms conformant to the FIPS standard 140-2. The embedded cryptographic algorithms has been validated with certificate #1747.

FIPS conformance will always be maintained when the following algorithms are used for establishment and encryption of the IPsec connection:

• Diffie Hellman Group: Group 2 to 14 (DH length of 1024 bits up to 2048 bits)

• Hash Algorithms: SHA1, SHA 256, SHA 384, or SHA 512 Bit

• Encryption Algorithms: AES with 128, 192 or 256 Bit or Triple DES

The respective modules can be configured in the IPsec Settings 162.

Profile Settings Backup

If a secure profile setting has not yet been generated, for example immediately after the software has first be installed on the computer, then the first profile settings backup is created automatically (NCPPHONE.SAV).

Create [Profile Settings Backup]

A profile setting backup will be created after each click on the "Create" menu item after a confirmation question. The backup contains the configuration up to this point.

Restore [Profile Settings Backup]

The last profile setting backup will be read in after each click on "Restore". Changes to the configuration that have been made since the last profile setting backup will be lost.

View

Via this feature you can modify the operating surface of the monitor and choose the language. The following features are found in the "View" pull-down menu:

Show Profiles

If several configured profiles are available, whatever is required can be selected from those lists.

Show Statistics

When "Show Statistics" is enabled additional information about the connection is displayed e.g. time online, transferred data, timeout etc.

Show Wi-Fi State

Independent of the communication medium of the current VPN profile you can enable a graphic display of Wi-Fi field strength if the Wi-Fi configuration has been enabled in the the monitor menu "Configuration / Wi-Fi".

The button [...] in this panel takes you directly to the configuration window of the "Wi-Fi settings".

If a mobile network card has been configured, then the menu item "Show Wi-Fi state" is inactive.

Show Tips

The tips give you important and quick information about configuring and customizing the monitor interface.

If you activate the tips, you will find a few important (15) key features of the client under the graphical display next to the company logo, which you can also replace (Tip 9).

Use the key combination [Ctrl] + [t] to scroll through the questionnaire.

With a mouse click on the question you get the answer.

Always on Top

When "Always on Top" is enabled the monitor will always be displayed in the foreground of your desktop regardless of what application is currently active.

Autostart

Use this menu item to select one of the following options:

• No Autostart: after the system has booted, the monitor has to be started manually.

• Monitor on the Desktop: after the system has booted, the monitor is started and displayed in its normal size.

• Icon in System Tray: after the system has booted, the monitor is started and minimized to an icon in the System Tray.

If you often require the use of the IPsec client and need the information displayed on the monitor, you should select the autostart option "Monitor on Desktop". However, it is not mandatory to have the monitor started in order to communicate with the remote gateway; none of the above settings impede the establishment of a VPN connection.

Minimize when Closing

Feature not enabled

If the monitor is closed via the close button [X] or by pressing [Alt + F4], the graphical interface (monitor) of the client is no longer displayed. If a connection is active the user will no longer see the connection status.

Feature enabled

If this menu item is enabled, the monitor is only minimized to system tray when closed via the button [X] or by pressing [Alt + F4]. It appears as a VPN icon in the system tray, showing the current state of connection.

Minimize when Connected

If this menu item is enabled the monitor will be minimized to system tray when the connection is established successfully.

GUI Scaling

Under tablets with higher definition the client can also be better operated on a touch screen, after it has been scaled to a manageable size.

A scaling degree of 150% is pre-configured and can be installed or de-installed again with a double click on the logo.

The display size in levels of 100, 125, 150, 175 and 200% can be variably set. A dynamic change to the scaling is possible with the key combination [CTRL] [+] or [CTRL] [-].

Note: The dialog necessary for connection build-up and statistics display have been optimised for scalable representation, but not for all configurations dialogs.

The setting are saved in the NCPMON.INI file under the following section:

[GENERAL]

Scaled=0

ScaleFactor=150

Language

The client software has been designed for international language support. The default language is English. In order to choose a language, click on "Language" in the view pull-down menu and then select the desired language.

Help

This menu item displays all available information on the client, regarding the help file, including the product description.

Further information on version and features of the current software are displayed under:

- [Logbook] 121
- [Extended Log Settings] 123
- [Client Info Center] 124
- [Network Diagnostics] 125
- [Search for Updates] 125
- [Activation] 125
- [Deactivate Client] 127
- [Info] 127

Logbook

Automised protocolling

The log function is continuously active in the background, even if the log window is not open. All relevant communication events of the client software are shown and saved for one week per operation day, in a log file. Files older than seven online days will be automatically deleted.

This log file is generated automatically in the installation directory under "Log" when the monitor ist finished and is named NCPyymmdd.LOG (yy=year, mm=month, dd=date).

The storage time for log files can be altered under Extended Log Settings.

The log files can be opened and analyzed with a text editor.

Selected Protocols

With opened log windows the current log messages are listed and can be followed. In this way the lines of the log protocol are automatically scrolled. The protocol created from the time of the opening of the log window until its closing is saved til the next re-boot. The contents of the log window manually can also be deleted, saved or searched through for specific events.

The following comands in the footer of the log window are prepared for these functions:

Create File

When you click this button, you receive the possibility to input name and path of a file in a further window, in which the content of the log window is written (default: ncpmon.log). All transaction with the client software, such as dialing and reception, including the numbers, are automatically protocolled and written in this file until the file is closed close. When you put in a log file, you can follow the transactions with the client for a longer period.

Close File

If you click on this button, a file with the log protocol of the window content is closed and saved under a free unused name. This file can be used for analysis of the transactions with the Secure Client or for error searches.

Clear Screen

If you click on this button the window from the last protocol entries will be emptied.

Close Logbook

The log window will be closed with this, without its contents being written in a file.

Show Search

Two search functions make the search for strings and expressions in the log protocol text easier to find.

Search

The string in the input field is searched for as it is in the log book and all the contained positions marked.

With [F3] you can jump from the chronologically oldest find spot with this string to the next latest, with Shift + [F3] you can go from the latest find spot to the next oldest.

Disable Scrolling

To stop the continuous reading in of the newer log messages you can set "Disable Scrolling ".

A search for more strings at the same time, is not possible.

Filter

After the string, which is input into this field, a search in the log text is carried out. Several strings can be separated or searched for at the same time, through gap characters. In the standard setting the lines with the relevant find spots are blocked out of the log protocol.

On the other hand only the lines can be shown where the filtered strings are situated.

Saving the search and filter entries

The history of the last 10 searches and filter entries will be remembered and shown in the selection list.

The maximum number of log lines, which are internally puffered is 1000 by default. This value can be changed via the NCPMON.INI.

The following values are saved in the NCPMON.INI for this function:

MaxTraceLines=1000

WholeWords=0

CaseSensitive=0

MaxSearchEntries=10

SearchEntry_X=X. Search String

MaxFilterEntries=10

FilterEntry_X=X. Filter String

Extended Log Settings

Additional log details can be collected for the following functions:

Client PKI Support

• PKI logs (PKI)

• PKI interface logs (GaCC)

Log settings for PKI modules are only written if they are enabled at this point.

Applications

• Client Monitor

• RWSCMD / NcpClientCmd

• Credential Provider

For the modulated applications mentioned here own log settings can be enabled if desired.

When extended logging is enabled, a flashing message is displayed in the Monitor; a double click on this flashing text opens the dialog for the Extended Log Settings.

When activating or deactivating logging for a service, that service must be restarted by pressing the corresponding "Restart" button.

Administrator rights are not required and the "Restart" button only restarts that service, not the system.

Client Info Center

The Client Info Center optimizes your support via User Helpdesk.

The overview supplies the following general information:

• Client Version (incl. Build Number)

• Current Connection Status (connected, disconnected, interrupted due to error)

• Client Service Status

• Current Certification Configuration (incl. Lifespan)

• VPN User ID

Furthermore informations are displayed on the following topics:

• Connections

• Services

• Certificate Configuration

• Network Adapters

This data can be exported to a text file by using the "Save to file" button in the Info Center's GUI. The information can also be exported independent of the monitor's operational state by entering the RWSCMD command: rwscmd /writeClientInfoCenterData [OutFileName].

Network Diagnostics

Network Tests are an option the Client Monitor's Help Menu and these can be used to test Internet availability. They support both PING to an IP Address in the Internet as well as resolution of an Internet Domain Name to an IP address. Domain names should be of the form "name.com".

Enter the address and press the corresponding Test button.

The test results are displayed via a symbol(success: green tick, failure: red cross) More details are displayed in a clear text log.

The tests are particularly useful for testing firewall rules for DNS requests and outgoing connections to the Internet.

Support Assistant

Use the Support Assistant to send the extended log data and any appropriate system information to the Support. Additional details such as screen shots can be attached as required.

After the automatic creation of an archive file (*Support.zip), the system e-mail program is used to e-mail the file to Support (support@ncp-e.com). Alternatively a browser can be started in which a form for support requests is displayed.

Search for Updates

Use this menu option to check whether a version of the software is available that is newer than the version installed. This can also be done when the free-traial software is still being used.

If a newer version is available, then a software update is always possible. Information on the features of the latest software version is always available on the web site.

Either configure the search cycle (never, daily, weekly, monthly) or press the "Search now" button.

Activation

The actual software version implemented, and where appropriate, the licensed version number with serial number, are shown under this menu option.

If the software is used under the free-trial license, then the remaining validity period is displayed in the pop-up window.

In order to use a valid full version that is not subject to time restrictions, the software must be activated using the license key and serial number purchased.

The licensing process for the software requires your acceptance of the license conditions; these conditions can be viewed via mouse click.

Free-Trial Version Validity Period

The free-trial version is valid for 30 days. Without software activation or licensing it will no longer be possible to set up a connection after this 30-day period expires. During this free-trial period press the activatiob button in the activation frame to initiate the licensing process.

After installation, each time the software is started the validity period will be shown in the pop-up window. Moreover, in a footer of the monitor the system will display how much longer the free-trail version can still be used, and when 10 days remain, a message box will be displayed to remind you that the software has not yet been licensed. This message box will appear once a day.

When the free-trial period has expired, the client software will only permit connections to be established to destination systems that are used for software activation/licensing. Thus one of the client's existing profiles will be used to set up an internet connection for licensing purposes.

Software Activation

The software must be either fully activated or de-installed when the free-trial period expires.

For activation, select the "License Data and Activation" menu option in the monitor "Help" menu.

The software version installed, together with the license in use is displayed here, i.e. you can see that the free-trial version has expired and that the software has not yet been activated/licensed.

Click on the license conditions to display the license agreement text. By activating/licensing the software you accept the license conditions.

The activation dialog can be opened by either clicking on the activation button in the in the monitor's tastbar or by selecting "Help / License Data and Activation" in the monitor menu. In the following screen you can select in which way the client should be licensed using a wizard.

Offline Version

In the offline version, a file that is generated after entering license key and serial number must be sent to the web server, and the activation key that is displayed on the website has to be entered in the licensing window of the monitor menu at a later point in time.

Online Version

In the online version, an assistant forwards the licensing data to the web server immediately after entry and thus the software is immediately released.

Deactivate Client

In order to be able to use a licensed version of the Client software, without restrictions, on another machine, the license details (serial number and license key) bound to the current hardware and operating system must be released at the Activation Server.

The user informs the Activation Server that the license will temporarily not be used by selecting "Deactivate Client" in the Help menu. In the input screen displayed, the user enters his/her name, optionally the name of the company and a valid e-mail address. When send is pressed, these details together with the serial number, license key and the language ID are sent to the Activation Server.

The Client is now deactivated; this is recognizable by the text "Software not Activated" displayed in a banner in the Client Monitor.

Subsequently the user will receive a mail with a URL link. When the URL link is opened in a web browser window, the license is reset at the Activation Server, i.e. the license details can then be used for activating the Client software installed on another machine.

Info

The info window shows product labels and version numbers.

Configuration Parameters

Available Profiles

The overview of "Available Profiles" lists, in three columns, information about those connection profiles that have been configured so far (Profile Name / Communication Medium / Standard). The column headings can be used to sort the profiles displayed and the checkboxes in the third column enable the configuration to be rapidly altered when using a Standard profile. The profiles do not need to be opened in order to change those profile settings.

Configuring the Profile Settings

The buttons (Add, Edit etc.) under the profile list cannot be used if the corresponding locks have been set. If there are no restrictions on setting profiles then all buttons will be operable and will call the associated functions.

In order to edit the (default) values in the profile settings, select the required profile and then click the [Edit] button.

The Configuration parameters are accessed via the following sub-menu:

Profiles [Parameters] 130
The IPsec configuration parameters are accessed by pressing [Edit] in the profile settings:

IPsec 162

Profiles [Parameters]

Select "Profiles" in the monitor menu and an overview of those profiles already defined is displayed. The buttons below the list are for modifying the profile settings.

In order to define a new profile, click on [Add] to start the "New Profile Wizard". Using prompts, this wizard requests you to enter only those parameters that are absolutely necessary and assists in the creation of a new profile definition; all parameters that are not requested will be assigned their default values.

The headline of the display shows the profile name and parameters defining that profile are located in various configuration folders. The names of the configuration folders are displayed on the left hand side:

Basic Settings [Profiles]

The client software enables individual profiles to be created and each can be configured according to user requirements. In order to distinguish between profile settings, allocate a name for the profile in this parameter field.

Please also refer to the following topics:

Profil Name [132]
Connection Type [132]
Communication Medium [133]
Default Profile after System Reboot [135]
Profile for Automatic Media Detection [136]
Microsoft Dial-up Networking [137]
Seamless Roaming [138]

Profile Name

When you define a new profile, you should initially enter a distinctive name for the profile (e.g. IBM London). The name may contain any desired letters as well as numbers and may be up to 39 characters including blanks.

Connection Type

Alternatively two connection types are available:

VPN to the IPsec correspondent:

In this case you connect with the company network (or with the Gateway) using the IPsec Client. For this purpose a VPN tunnel is set up.

Internet connection without VPN:

In this case you use the IPsec Client only for the dial-in to the Internet. In the process Network Address Translation (IPNAT) will be further used in the background so that only data packets which were requested are accepted.

Communication Medium

You can select the communication medium for each profile, providing you have the required device installed on your PC and recognized by Windows. The following communication media can be selected:

LAN (over IP)

Hardware: LAN adapter;
Networks: Ethernet based LAN;
Remote Destination: Remote destination of local multi-protocol router in the LAN

Mobile Network

If a cell phone is to be used (mobile network) then this communication medium may be selected.

Wi-Fi

Hardware: Wi-Fi adapter;
Networks: Wi-Fi;
Remote destination: Access Point;

The "Wi-Fi Settings" are accessed by selecting the "Configuration/Wi-Fi" monitor menu. If Wi-Fi is to be enabled and managed by the Client software then tick the "Enable Wi-Fi Configuration" checkbox; control of the Wi-Fi interface adapter is then performed by the Client software and the operating system Wi-Fi management tool is disabled. (Alternatively the management tool of the Wi-Fi card can be used; in this case the "Enable Wi-Fi Configuration" option in the "Wi-Fi Settings" menu must be deactivated.)

Using the Wi-Fi Settings menu, access data for wireless networks can be saved in individual Wi-Fi profiles.

If the connection type Wi-Fi is set for a destination system in a particular VPN profile setting, then under the Client Monitor's graphic frame an additional frame displays the Wi-Fi network in use, together with its field strength.

automatic media detection

If different communication media are to be used alternatingly, e.g. LAN or Wi-Fi (within the corproate network) or Mobile Network, manual selection of the profile with the corresponding communication medium is rendered superfluous, provided the profile with communication medium LAN has been changed to a profile with automatic media detection and a profile for each alternatively available communication medium like Mobile Network is available.

The profile with automatic media detection has to be configured with all parameters necessary for the connection to the VPN gateway. (The configuration has to contain the Gateway (Tunnel Endpoint) 165).

The alternative profiles have to include the respective communication medium and the following paramter fields have to be configured: "network dial-in" - access data for the internet service provider; "basic settings" - profile for automatic media detection.

Prior to connection set-up, the profile with the communication medium automatic media detection has to be selected. If this is the case, the client automatically recognizes the communication media available and selects the fastest of all available profiles.

Configuration Instructions:

1. Configure a profile for LAN or Wi-Fi to the VPN gateway within your corporate network. For this you need the IP address of the VPN gateway and your authentication data (i.a. VPN user ID; VPN password) and possibly the certificate configuration.

2. Change the communication medium from LAN or Wi-Fi to "automatic media detection". (A connection to the VPN gateway within the corporate network has to be possible with this configuration!)

3. Configure an alternative profile which contains all access data for the internet service provider and the parameter for an alternative communication medium. Then define this profile as "profile for automatic media detection". (The use as profile for "Automatic Media Detection" can also be selected in the profile selection)

4. The alternative profile may be copied for further alternative communication media. Only media specific parameter changes need to be made in these profiles.

5. Please take care, that prior to connection set-up the profile with the communication medium "automatic media detection" has to be selected.

Default Profile after System Reboot

Normally after a system reboot the Client Monitor is opened with the last profile used. If this "Default Profile after System Reboot" function is activated, then after a system reboot, the profile defined will always be loaded, independend of which profile was last used.

Profile for Automatic Media Detection

A tick in this box indicates that this profile is to be assigned to automatic media detection. If the associated communication media is currently available, this profile will be used automatically for establishing a connection. Please refer to the description under [Communication Medium] 133.

If this function is switched off (the check mark is removed), then this profile can also be selected manually in order to set up a connection, so long as the tunnel parameters for access to the VPN Gateway have been entered correctly.

If a destination system or a profile with the communication medium mobile network should be used for automatic media detection, the SIM PIN of the card has to be entered in the configuration under "Connection / Mobile Network".

Microsoft Dial-up Networking

For the dial-up on the ISP (Internet Service Provider) the microsoft remote transmission dialer can be used. This is always necessary when the dial-up point requires a dial-up script. The remote transmission dialer supports this script. In the parameter window "Network dial-up" the script file is subsequently entered by inputting the path and name of the script file which is running (see below script file).

never

With the "Never" setting the dialer of the client is used exclusively to dial-in.

only for script dial-in

If the data communications dialer is used "only for script dial-in", then select this option. For a dial-in point that does not require a script, the system automatically switches to the dialer of the client.

always

If the data communications dialer is always used, then the appropriate setting has to be made.

In the parameter folder "Dial-up Network" the RAS script file must be entered including its path and name. The script file you receive from your provider.

(Using an international phonebook the script file is entered automatically and cannot be modified anymore.)

Seamless Roaming

Seamless Roaming is configured by using two Link Profiles in the Profile Settings. The communication medium of one Link Profile with a LAN connection to the gateway is changed to "Automatic Media Detection" and the switch "Seamless Roaming" set; a connection to the gateway via mobile network is defined in a second Link Profile and this is activated with "Profile for Automatic Media Detection"

If a Wi-Fi profile with hotspot configuration is also available and the connection from the mobile network card has been made, the client will automatically attempt to establish the connection in the sequence LAN, Wi-Fi, Mobile Network, always using the fastest medium available.

In this case it is important to note that abnormal roaming charges could be incurred, dependent on the medium used.

(Seamless Roaming is only supported under IKEv1 based connections.)

Seamless Roaming is performed automatically, in the background, between LAN, WLAN and Mobile Network connections, when the Internet connection of one of these media fails and is interrupted. In such a case the Secure Client automatically switches to the next available medium; faster connection media always have priority.

This seamless change of connection medium has the effect of simulating an always-on function. Applications using the VPN tunnel are unaffected by the automatic change of the physical connection medium. The logical connection remains in place during any potential pauses in connection caused by re-connecting the next physical connection.

Dial-up Network

This folder contains the User ID and Password required to correctly identify the user when accessing the destination system. These two parameters are needed for the PPP negotiation to the ISP (Internet Service Provider).

Please also refer to the following topics:

User ID [Dial-up Network] 139
Password [Dial-up Network] 140
Save Password 141
Destination Phone Number 142
RAS Script File 143

User ID [Network Connection]

This parameter is used for identifying yourself to the remote Network Access System (NAS) when establishing a connection to your Destination, or alternatively to your Internet Service Provider (ISP) if you are communicating across the Internet. The User ID can include up to 254 characters. Normally the User ID will be assigned to you by your Destination, e.g. your company Headquarters, Internet Service Provider or User Help Desk.

It must be supported and accepted by the NAS, RADIUS or LDAP Server for Authentication purposes.

Password [Network Connection]

You need the password to be able to identify yourself to the Network Access Server (NAS) when the connection is established. The password may be up to 128 characters long. In the normal case, you will be assigned a user name from the target system, since you must also be recognized from there. You receive it from your head office, from the Internet Service Provider or the system administrator.

Note: If profiles are configured for the "automatic media detection", it is compulsory that a (NAS) password be entered for all of these profiles, otherwise the connection cannot be established.

Upon entering your Password all characters will be displayed as an asterisk (*) in order to keep them from being detected by someone else. Therefore it is necessary to be very careful that you enter your password exactly the way in which it was assigned to you (also with regard to upper case and lower case characters).

Note: It is not mandatory to enter your password in the profile settings. If, however, you have defined "Automatic" as your communication medium, you have to execute your initial (first) connection manually under these circumstances . Upon doing so the Secure Client will prompt you for your password. Thereafter any automatic reconnections that are executed will refer to this password until such a time that you (re) boot your PC or until you change your destination.

Save Password

This parameter should be activated when it is desired that the Password (if entered) be stored. Otherwise it will be deleted when (re)booting your PC or changing your destination. Under normal circumstances you will want to have this field activated (this is also the default setting).

Important: For security reasons you must be aware that should some unauthorized person use your PC, they will be able to use your password. Therefore caution should be used when your PC is unattended.

Destination Phone Number

You must define a phone number for each destination otherwise the client will not be able to dial-up and establish a connection to the destination. The phone number must be entered exactly in the same manner as if you were dialing the number from a telephone. You must enter any required prefixes, outside line prefix, country codes, area codes, extensions, etc. etc.

Example: Making a connection from Germany to UK:

Enter: 00 (gets you an international line when dialing from Germany)

Enter: 44 (this is the country code for United Kingdom)

Enter: 171 (prefix for London)

Enter: 1234567 (the number you want to call)

The following number will be used by the client for dialing purposes and it will be displayed in the profile as follows: 00441711234567

The destination phone number may include up to 30 characters.

Alternative Destination Phone Numbers

It could be that the destination you want to communicate with uses a Network Access System (NAS) that is equipped with multiple individual phone numbers. If this is the case, it may be useful to enter more than one telephone number for the destination if for example the primary destination phone number is occupied. The alternative destination phone number(s) must be entered immediately following the primary destination phone number and be separated by a colon (:) or semi-colon (;).

The Secure Client supports a maximum of 8 alternative phone numbers.

Example: 00441711234567:00441719876543

The first number is the primary destination phone number and will always be dialed first. The second number is the alternative destination phone number and will be dialed when a connection to the primary number is not possible.

Important: This will only work if the protocol settings associated with alternative destination phone number are the same as the primary destination phone Number.

RAS Script File

Using Microsoft's RAS Dial-up Networking the RAS Script file including its path and name must be entered.

Mobile Network Configuration

This folder contains the communication media parameters used to establish a connection to the Internet gateway. There are three different configuration modes:

Configuration mode

automatic

In the default mode, "automatic", the APN details are read from the SIM card. When "automatic" is selected, all fields from the current provider configuration are deleted. The driver then uses the NetID from the SIM card to search the APN.ini file for the associated APN details.

Provider List

Alternativly the provider required can be selected from a "Provider List". (If your provider is not listed, the list can be extended with the details of your provider; edit the APN.ini file in the installation directory).

user-defined

In "user defined" mode, the user is responsible for entering all data manually.

Country

In the "Provider list" mode, select the country in which you are currently located; the most important providers will then be displayed. The Provider List is editable and stored as APN.ini in the installation directory.

Provider

In the configuration mode with the Provider List, the most important providers in a particular country can be selected. (If your provider is not listed in the display, the list can be extended with the details of your provider; edit the APN.ini file in the installation directory). When a provider is selected the associated parameters, when present in the list, are automatically set into the configuration.

APN

You obtain the APN (Access Point Name) from your provider. It can either be entered manually or read from the provider list. It is "web.vodafone.de" for Vodafone and "internet.t-d1.de" for T-Mobile. The APN is usually used for administration purposes.

Dial-up Number

Enter a defined string of characters as "dial-up number" depending on your SIM card and provider. This string of characters tells the Mobile Network card which type of connection has to be set up. Usually this string is *99#. (If the connection cannot be established, please contact the hotline of your service provider).

Authentication

Different wireless network providers use different protocols for authenticating connections from mobile devices to their network. PAP and CHAP are the two most commonly used, but the protocols can also be selected automatically and dynamically when the Mobile Network connection to the Internet is being established.

In "manual" mode, select the protocol - PAP or CHAP - defined by the provider. If authentication is not specified by your provider, leave this setting in its default "automatic" state.

User ID, Password

Enter user ID and password, both of which can be freely assigned and function as access data for your ISP. This only applies if you use the automatic mode or the user defined configuration mode. If you have received a specified user ID and password from your service provider, use these. With Vodafone and T-Mobile any string of characters is sufficient.

Forced Password Prompt at Mobile Network Connection Setup

Usually, no specific user ID or password are required when setting up an Internet connection via mobile network. If the mobile network connection requires the user to enter a user ID or password, because the company's internet access has an APN or provider of its own, for example, the user identification prompt can be automatically displayed in a new window.

In order to use the forced password prompt, enter <pwreq> (including angle brackets) in the password configuration field in the mobile network configuration.

SIM PIN

Use a SIM card for mobile networks or enter your PIN for this card in this field. If the SIM PIN field is left empty, the SIM PIN will be prompted for when using this profile to establish a connection. Decide whether or not the SIM PIN is to be saved for this profile.

If you use a cell phone, the PIN will already have been entered when switching the phone on.

HTTP Logon [Profiles]

The settings in this parameter folder are used to carry out the automatic HTTP Logon. A centrally created logon script with its associated logon data can be be used to establish a connection to the access point (hotspot) without having to open a browser window.

The automatic logon to a hotspots works as follows: once a connection to the the access point has been established, an HTTP redirect from the client to the associated website is executed. Instead of having to start a browser for HTTP authentication, the authentication occurs automatically in the background, using the entries made here.

Note: the connection via a hotspot will usually be subject to a fee. You must agree to the terms and conditions of the hotspot operator if the connection is to be established.

For the script-controlled logon a script from the installation directory

<install>\scripts\samples

can be adapted as necessary for other hotspots.

See also the parameters:

User ID [HTTP Logon] 147
Password [HTTP Logon] 147
HTTP-Authentication Script [HTTP Logon] 147

User ID [HTTP Logon]

This is the user ID provided by the hotspot operator.

Password [HTTP Logon]

This is the password provided by the hotspot operator. The password is concealed with asterisks (*) when entered.

HTTP Authentication Script [HTTP Logon]

Click on the [Browse]-button to select the saved logon script.

In order to check incoming certificates using HTTP authentication, the variable CACERTDIR must be set in the script. To check the other contents of the Web Server certificate, the following variables must be used:

CACERTVERIFY_SUBJECT: checks the contents of the subject (e.g. cn=WEB Server 1)

CACERTVERIFY_ISSUER: checks the contents of the issuers

CACERTVERIFY_FINGERPRINT: checks the MD5 fingerprint of the issuer certificate

If the contents do not match the certificate, the SSL connection will not be established and a log message will be send.

Script for Vodafone WebSessions

If mobile internet access for Vodafone WebSessions is to be used, only the Vodafone WebSession SIM card for the 3G card has to be installed and a profile with the connection type Mobile Network set up.

For "HTTP Logon" select the HTTP authentication script, corresponding to your planned Internet use

(30 minutes = vodafonewebsession30m.nhs,

1 hour = vodafonewebsession01h.nhs,

24 hours = vodafonewebsession24h.nhs).

In the profile settings in Mobile Network Configuration 144 the user defined APN has to be "event.vodafone.de" and the dial-up number "*99#".

After connection setup and entry of suitable access data direct Internet access will be available.

Line Management [Profiles]

In the "Line Management" folder define the connection mode, together with any timeout values that will specify when a link is to be automatically disconnected.

Please also refer to the following topics:

Connection Mode [Line Management] 149
Inactivity Timeout [Line Management] 150
Disconnect the logical VPN tunnel when the connection is broken 154
Prioritize Voice over IP (VoIP) 154
Enable Tunnel Traffic Monitoring 155
Alternative IP Address 156
Quality of Service (Profile) 157

Connection Mode [Line Management]

Define here how and when connections are established:

manual

The default setting for Connection Mode.

When Connection Mode is set to "manual", VPN connection establishment has to be activated manually (by pressing Connect). The connection will be disconnected on expiry of the inactivity timeout provided that this parameter has been set to a non-zero value (0). If the inactivity timeout is set to zero then the connection must be manually disconnected.

automatic (connection initiated by data transfer)

If this mode is selected, VPN connections are established automatically whenever data transfer to a remote host is initiated by a Client application. How the connection is disconnected is dependent on how the Client is configured, i.e. according to application requirements and profile settings.

Important: when connection mode is configured such that connections are established automatically, then the password for the connection must be entered, otherwise the connection will not be successfully established.

always

When Connection Mode is set to "always", a VPN connection is always established automatically when the Client starts. Connection establishment is independent of the "Connect" button, of the onset of data transfer, or of how the monitor is set to be displayed - see Autostart.

variable (Connect starts automatic mode)

If this mode is selected, the first VPN connection must be established manually (by pressing "Connect").

How subsequent connections are established is dependent on how the previous connection was disconnected:

• if the connection was disconnected by a timeout, then the next connection will be automatically established whenever data transfer to a remote host is initiated by a Client application.

• if the connection was disconnected manually (by pressing "Disconnect"), then it must be reestablished manually.

If the timeout is set to zero (0), i.e. no timeout is set, then the connection must be disconnected manually.

Important: If "Connection Mode" is set to "manual", then activate a timeout (i.e. set timeout to non zero) in order to automate disconnection, otherwise unnecessary connection costs could arise.

variable (Connect starts always mode)

If this mode is selected, when "Connect" is pressed to establish a VPN connection the Client starts using the "always" mode - see "always" above. The Client continues using "always" mode until the monitor is closed, when the mode reverts to this setting.

Inactivity Timeout [Line Management]

This parameter is for setting the time delay to be used following the last transmission of data before automatically executing disconnect. Time is expressed in seconds. Possible settings are from 0 to 65356 seconds.

If your communications connection (regardless of communication medium) receives a charge/unit impulse from the network provider, this will be used by the Secure Client timeout feature for achieving an optimal disconnect time with regard to the value set in the inactivity timeout. This optimized timeout feature will further help to reduce communication costs.

Note: In order for the inactivity timeout to be activated it is necessary to enter any value from 1 to 65356. The value "0" (zero) means that no automatic timeout (disconnect) is executed. When the inactivity timeout is set to "0" (zero) you must manually execute disconnect.

Important: The inactivity timer only begins counting down after the last data transmission and after any communications handshaking has stopped.

Timeout Direction

With this parameter you determine for which transmission direction the timeout should apply. Three different settings are possible:

TxRx (default):

The client observes both, the end of the sent (out) as well as the received (in) data, before the timer begins counting down.

Tx:

Only the sending direction (out) is observed.

Rx:

Only the receiving direction (in) is observed.

OTP Token

If a one-time-password (OTP) token is used, the PIN and one-time password of the token can be entered and used instead of the default "User ID" and "Password".

The use of the OTP is defined as follows:

off

(default) OTP is not used

NAS Dial-up

If the OTP Token is to be used for accessing a NAS, then the "Password" parameter field located in the parameter folder "Dial-up Network" is set to inactive.

VPN Dial-up

If the OTP Token is to be used for accessing the VPN gateway, the "VPN Password" parameter field located in the "VPN parameter" folder is set to inactive.

When dialing-up, a dialog window is displayed prompting for the "One-time password for VPN-Access", which requires the PIN and one-time password to be entered.

If messages are sent from the ACE server because of the RSA token, then these messages are displayed on the monitor in an input field (for example "Expiration of the valid PIN"). In this case, enter the new PIN or the new password from your token into the respective field.

Swap OTP and PIN

This expert parameter should only be set by an experienced system administrator who is informed about the system architecture of the two-factor authentication used.

When establishing a VPN connection, a pop-up window is displayed, which always polls three authentication parameters in the same order:

– User Name (VPN User ID)
– PIN (PIN for using an RSA Token)
– One-Time Password (OTP)

PIN and one-time password are concatenated to a VPN password in string form when they are sent to the OTP server. The sequence of the combination of PIN and one-time password must meet the requirements of the respective OTP server. The RSA Authentication Manager (SecurID Server) usually expects a VPN password according to the standard pattern "PIN + one-time password".

If the RSA Authentication Manager or OTP server expects a result that corresponds to the pattern "One-Time Password + PIN", this result can be generated by activating the configuration option "Exchange one-time password and PIN".

Note that this parameter has no effect on the concatenation of the authentication codes on the display in the pop-up window interface.

Hide Username when Prompted for Credentials

During the re-establishment of a VPN connection with manual input of the access credentials (after the previous VPN connection was disconnected), the user can be forced to re-enter the username in order to successfully establish the new VPN connection. To force this behavior, enable this parameter. The parameter is effective both on the credentials dialog and during Windows pre-logon.

If this parameter is disabled (default setting) then a user only has to enter the correct password in order to establish a VPN connection; the username, cached from the previous connection, is re-displayed and the user does not have to re-enter it. While this default setting maintains compatibility with previous versions, security breaches could be initiated by "stealing" the username while it is displayed during the credentials prompt.

If this parameter is enabled, it ensures that each attempt by a user to establish a VPN connection is fully authenticated using the full credentials that have been made available only to the authorized user.

Disconnect the logical VPN tunnel when the connection is broken

This switch modifies the default behavior of the Client

(maintain logical connection)

If the Client's default setting is switched off, the logical connection will also be disconnected when the physical connection breaks, and the VPN tunnel will be disconnected.

Important

The behavior of Seamless Roaming is independent of the setting of this switch; as soon as a connection is established using a profile that incorporates Seamless Roaming, the logical connection is preserved across breaks in the physical connection and only disconnected when that profile's VPN connection is disconnected.

Only when Seamless Roaming is not being used does the setting of the default behavior have an effect on the behavior of the logical connection.

Visual Feedback about Status of Tunnel

When a break occurs in the physical communication medium connection used to establish a VPN tunnel, the existing VPN tunnel remains established, for an unspecified length of time. Thus the tunnel remains logically active while the new physical connection is being established.

During the period the physical connection is broken, the normally solid green bar displayed in the Client monitor changes to a dashed green bar and the icon in the system tray flashes yellow and green. These indicators remain until the physical connection is re-established, when they return to solid green.

The monitor does not show the dashed green bar if the Client's default behavior is switched off and a profile without Seamless Roaming is used for connection establishment.

Prioritize Voice over IP (VoIP)

Should this client be used for communication with Voice over IP, this function should be activated in order to send and receive the speech data without delays or distortions.

Enable Tunnel Traffic Monitoring

In locations with poor mobile wireless reception, there is a chance that despite a VPN tunnel being established and a green bar being displayed in the Client monitor, data cannot actually be transferred across the tunnel. In order to give the correct feedback to the user in such a situation, "Tunnel Traffic Monitoring" can be enabled.

PING to Tunnel Endpoint

When this option is enabled a configurable target address in the remote network is automatically pinged periodically. By default the VPN tunnel's Gateway (Tunnel Endpoint) 165 is pinged. If another address should be used, this can be configured in the Alternative IP Address 156 field.

If the ping is not correctly answered, the monitor's tunnnel status bar changes from continuous green to dashed green and the message "VPN internet connection is temporarily broken" is displayed in the Windows Notification Area.

The faulty VPN tunnel is then disconnected and an attempt is made automatically to reestablish the VPN tunnel.

Alternative IP Address

By default Tunnel Traffic Monitoring will ping the VPN tunnel's Gateway (Tunnel Endpoint) 165. If, however, an alternative address should be ping'd to test that the VPN tunnel is correctly established - for example an address that can only be reached when a VPN tunnel is established - enter the corresponding IP address in this field.

Permit IP Broadcast [Advanced]

You decide with this parameter whether the client software should allow the transmission of IP broadcasts. IP broadcasts are used for example if a LAN client (such as the client software) searches for a file server on the network. In the case of the client the network would be a remote LAN, to which the client is connected.

IP broadcasts are disabled if the field is not checked (default setting).

IP broadcasts must be permitted if DHCP is in use, in order for DHCP to be able to request an IP address of the destination system.

Quality of Service

Select here a VPN profile for which a configuration of Quality of Service 77 is to be used.

The configuration of Quality of Service will be effective immediately after the VPN connection is established with this profile to the gateway.

(During the active connection the QoS groups can be switched on or off for test purposes under "Connection Info 29".)

Extended Authentication [Pre-authentication]

Various authentication procedures may be required before the VPN connection is established.

Biometric Authentication

Windows Hello allows different types of biometric authentication.

Please see Fingerprint / Biometric Authentication 159.

Fingerprint / Biometric Authentication

When this setting is enabled, an authentication prompt is displayed as soon as the user clicks connect in the client. The VPN connection will only be initiated after successful authentication via the method configured for Windows Hello (fingerprint recognition, face recognition, PIN entry, etc.).

If the option "Fingerprint / Biometric Authentication" is activated, "Windows Hello" must be preconfigured accordingly.

Please note the detailed description Biometric Authentication 205.

EAP Authentication [Pre-authentication]

If the client is to use EAP (Extensible Authentication Protocol) for authentication, this function has to be activated. It has the effect that the EAP configuration set in the monitor menu under EAP Options is used for this profile.

Note: the EAP configuration in the monitor menu is valid for all profiles and has to be activated if this link-specific setting is to be effective.

EAP is used if a Wi-Fi access point is used which is capable of 802.1x and demands a corresponding authentication.

EAP can also be used if the client wants to access another network segment of the company network by means of a router.

EAP generally prevents an unauthorized user from logging into a LAN via the hardware interface.

After configuration of the EAP, a status messages should be displayed in the graphics frame of the monitor. If this does not happen, switch on the EAP Configuration in the monitor menu. EAP can be restored by means of a double click on the EAP symbol. Subsequently the EAP negotiation takes place again.

HTTP Authentication [Pre-authentication]

This function has to be activated to enable automatic HTTP authentication at the access point (hotspot).

In this way a further configuration folder is added in the profile settings, in which the authentication data can be entered (see HTTP Logon 146).

In the event of a link with the connection type Wi-Fi, the HTTP Logon is not swiched on!

Instead the activation of this function has the effect that for this profile the authentication data from the Wi-Fi settings in the monitor menu are used.

Note: The connection via hotspot provider is usually a chargeable service and you must accept the hotspot provider's licensing terms before the connection is established.

IPsec Settings

Enter the IP address of the IPsec gateway in the corresponding field. In addition, select the policies to be used for negotiations carried out as part of the tunnel establishment procedure.

When, instead of a specific policy, "automatic mode" is to be used (by selecting "automatic Mode" from the pulldown list), the client and the IPsec gateway will negotiate the use of a proposal from a list of proposals sent by the client. If "automatic mode" is selected then the policy must be chosen in coordination with the remote gateway; select the required policy from the pulldown list.

The following policies are delivered with the software:

IKEv1 Policy

The pulldown "IKEv1 policy" list also includes the "Pre-shared key" and "RSA signature" policies, select one of these instead of the default "automatic Mode" setting.

IKEv2 Policy
Alternatively, IKEv2 policies are also provided.

IPsec Policy

The pulldown "IPsec policy" list also includes the "ESP - AES128 - MD5" policy, select this instead of the default "automatic mode" setting. (See also the guidelines for policies / proposal lists for IKE and IPsec policies).

The pulldown "IPsec policy" list also includes the "ESP - 3DES - SHA" policy, select this instead of the default "automatic mode" setting. (See also the guidelines for policies / proposal lists for IKE and IPsec policies).

See also the following:

Gateway 165 (Tunnel Endpoint) 165
Exch. Mode [Profiles] 166 IKEv2 Policy [Selection] 173
IKE DH Group [Profiles]
IPsec Policy [Selection] 175
PFS Group [Profiles] 178
Lifetime 179

As a rule, the policies will only require reconfiguring when there is no proposal in the client's policy (proposal list) that exactly matches the IKEv1, IKEv2 or IPsec proposals at the gateway.

IPsec Configuration

Use the [Policy Editor] to open the "IPsec Configuration".

The "IPsec Configuration" (Policy Configuration) will display the following folders. The folder displayed is dependent on which of IKEv1 or IKEv2 has been selected under "IPsec General Settings". Policies can be added or modified.

The IPsec Policy folder contains the policy "ESP-AES128-MD5".

Editing Policies

To edit the (default) values of a policy, i.e. to set or modify parameters in a proposal to make it conform to the requirements of the IPsec gateway. Using the mouse, select the policy folder to which the proposal belongs. Only then can any changes be made. Press the appropriate button. [Edit], [Copy] and [Delete] buttons will have become active.

Edit

If required, use [Add] to add a new proposal and use the pulldown lists to select the proposal details required, or use [Remove] to delete an existing proposal (note that a policy must have at least one proposal).

Add

If required, use [Add] to add a new proposal and use the pulldown lists to select the proposal details required, or use [Remove] to delete an existing proposal (note that a policy must have at least one proposal).

Copy

To copy the parameter settings of a policy which has already been defined, mark the policy to be copied and click on [Copy] which opens the parameter folder. Now change the name and then click on [OK]. The new policy has now been created. The parameter values are identical to those that were copied except for the name, select the proposal details required.

Delete

To delete a policy from the policy folder, select it and click on [Delete]. The policy will now have been permanently deleted from the IPsec configuration.

Close

Press [Close] to close the IPsec Configuration folder; the configuration parameters are stored and you return to the monitor.

Save

Every change to an IPsec or IKE Policy is saved by pressing [OK]. This returns you to the IPsec Configuration folder.

Policy Lifetimes

The policy life time parameters apply for all policies of a profile, IKE, IKEv2 and IPsec policy. Use [Policy Lifetimes] to open the Policy Lifetimes folder and modify the parameters as appropriate.

Further information about FIPS see: FIPS Certification 11

Gateway (Tunnel Endpoint)

Enter the address of the remote gateway here. You will receive that address from your administrator, either as an IP address or as a name string.

IP address

If the gateway is equipped with a static, official IP address, enter that IP address.

Either the IPv4 or IPv6 protocol can be used to communicate between the Client and the VPN gateway. The IP address entered in this field must conform to the IPv4 or IPv6 address formatting rules, as appropriate. These rules are as follow:

IPv4 (32 bit address):
the address must be in the dotted decimal notation e.g. 15.168.1.253

IPv6 (128 bit address):
the address must be in the hexadecimal notation (8 groups of 4 hex characters, separated by colon) e.g 2001:0db8:ac10:002b:0000:0000:0000:0002

Shortened representations are allowed:
Leading zeros can be suppressed e.g. 2001:db8:ac10:2b:0:0:0:2
Multiple zero groups can be concatenated to colon colon, e.g. 2001:db8:ac10:fe01:2b::2

Name string

If the gateway does not have a fixed IP address, then enter the name string provided by the Internet Service Provider. This is the fully qualified domain name of the gateway, stored in the Service Provider's DNS.

Notes

Alternative tunnel endpoints can be entered in addition to the first tunnel endpoint. The addresses must all be separated by comma (,) or all by semicolon (;). Spaces are not allowed as separators.

A maximum of four different tunnel endpoints may be defined in the Client for use in connection establishment. These will be selected as follow:

1. If the alternative tunnel endpoints are separated from each other by a semicolon (;), attempts to establish a connection will made in the sequence of tunnel endpoints, starting with the first entry in the list. If that attempt fails, the next address in the list will be used and the process will be repeated by the Client for a maximum of seven successive attempts or until a connection attempt is successful.

2. If the alternative tunnel endpoints are separated from each other by a comma (,), attempts to establish a connection will made in the sequence of tunnel endpoints, but the address of the first attempt will be chosen at random. If that attempt fails, the next address in the list will be used and the process will be repeated by the Client for a maximum of seven successive attempts or until a connection attempt is successful.

Exchange Mode [Profiles]

Main Mode (IKEv1):

In Main Mode (default setting) six messages are sent over the Control Channel and the last two messages are encrypted. The last two messages contain the user ID, the signature, the certificate and, if required, a hash value. This is why it is also known as "Identity Protection Mode".

Aggressive Mode (IKEv1):

In Aggressive Mode only three messages are sent over the Control Channel and nothing is encrypted.

IKEv2:

The Internet Key Exchange Protocol Version 2 (IKEv2) includes the Mobility Extensions (MOB IKE) in the Client's base.

Tunnel IP Version

This parameter can be used to configure for which IP version the IPsec negotiation should be performed. The configuration option exists only for IPsec connections with key exchange via IKEv2!

Only if the Exchange Mode IKEv2 ⌐166⌐ is set, this option is displayed to select the tunnel IP version:

IPv4

Is the default setting (this ensures that the VPN client behaves exactly the same way after a software update).

IPv6

If the gateway of a third-party manufacturer supports IPv6, this setting can be selected. VPN gateways from other manufacturers, which do not support IPv6 but receive IPv6 packets, behave differently and may not build a tunnel. Therefore, it is recommended that you do not configure IPsec negotiation for IPv6 in this case.

IPv4 + IPv6

With this setting, for example, a network architecture can be supported whose gateway (destination address) only supports IPv4, but the devices of the company network IPv6.

Policies

IKEv1 and IKEv2 Policies [Profiles]

IKEv1 Policy

Select the IKEv1 policy from the pulldown list (preconfigured: "Pre-shared Key" and "RSA Signature"). All IKEv1 policies which were created during software installation or during IPsec configuration are listed by name in the pulldown.

automatic Mode: In this case it is not necessary to configure the IKEv1 policy in the IPsec menu.

Pre-shared Key: This preconfigured policy can be used without PKI support. The same "Static Key / Pre-shared Key" must be used at both ends of the VPN link.

(See Pre-shared key / Shared secret in the Identities 183 configuration folder).

RSA Signature: This preconfigured policy can only be set if a PKI has been implemented (Secure Server). Implementation of the RSA signature as additional strong authentication requires the use of a smartcard or soft certificate.

If the Secure Entry Client is to use special IKEv1 policy proposals or lifetimes, use the [Policy Editor] and [Policy Lifetimes] buttons to create, modify or delete the respective details.

IKEv2 Policy [Profiles]

If the Secure Entry Client is to use special IKEv2 policy proposals or lifetimes, use the [Policy Editor] and [Policy Lifetimes] buttons to create, modify or delete the respective details.

If automatic mode is selected, it is not necessary to configure an IKEv2 policy.

Important: If IKEv2 has been selected as the key exchange protocol, by selecting IKEv2 as the "exchange mode", an IKEv2 authentication protocol must be selected - see "IKEv2 Authentication".

IKE DH Group [IKE Policy]

The selection of one of the Diffie Hellman groups offered determines the level of security for the key exchange. Later a symmetrical key will be generated according to this selection. The higher the DH Group the more secure the key exchange.

By a mouse touch a tool tip with the corresponding RFC standard appears for the selected group.

The default is DH19.

IKEv1 Policy [IPsec Configuration]

The parameters in this folder apply to the Internet Key Exchange (IKE) with which the control channel for the SA negotiation is established.

The IKE policies which you configure here will then be listed for selection in the "IKEv1 Policy" pulldown in the IPsec General Settings folder.

Two IKE policies are delivered with the software and they provide differing functionally: "Pre-shared Key" and "RSA-Signature". Every policy lists at least one proposal for authentication and encryption algorithms (IKEv1 policy, authentication, encryption), i.e. a policy consists of one or more proposals.One IKE policy is delivered with the software: "Pre-shared Key". Every policy lists at least one proposal for authentication and encryption algorithms (IKEv1 policy, authentication, encryption), i.e. a policy consists of one or more proposals.

The same policies including the associated proposals should apply for all users, meaning that the same proposals should be configured in policies, both on the client side and on the VPN gateway.

Algorithms and Parameters

The following policy/proposal parameters are common to all connection profiles:

Name [IKEv1 Policy] [170]
Authentication [IKEv1 Policy] [170]
Encryption [IKEv1 Policy] [170]
Hash [IKEv1 Policy] [170]

Name [IKE Policy]

When adding a new policy, first give it a name by which it can be referenced later.

Authentication [IKE Policy]

Open the proposals folder by clicking on the "Proposal" tab. The two sides of the VPN link must have authenticated each other before the Control Channel for Phase 1 negotiations (IKE Security Association) can be established.

Pre-shared Key

Select this setting if the same pre-shared key (also referred to as the shared secret) is to be used on the client and the VPN gateway for mutual authentication. Define the "Shared Secret" key to be used in the Identities [183] configuration folder.

RSA Signature

Select this setting if details from a certificate, configured for the "Extended Authentication" (XAUTH), are to be used for mutual authentication.

(In Main Mode the certificate will also be encrypted. Note: only select "RSA Signature" if a PKI infrastructure is in place.

Encryption [IKE Policy]

Symmetrical encryption of messages 5 and 6 in the Control Channel occurs according to one of the optional encryption algorithms if Main Mode (identity protection mode) is used. In automatic mode the encryption is determined by the communication partner.

For each IKE policy proposal, a custom encryption algorithm can be selected from the pull-down menu.

Hash [IKE Policy]

This is the mode that determines how the hash value over the ID is formed, or in other words how the certificate of messages is formed in the control channel.

From the displayed list a value can be selected.

IKEv2 Authentication [Profiles]

In contrast to IKEv1, IKEv2 mandates that initiator (the Secure Client in this case) and responder (the VPN gateway) must mutually authenticate each other, i.e. Client → VPN gateway and VPN gateway → Client.

At the client side one of three different IKEv2 authentication methods can be chosen:

Certificate

Select the appropriate certificate via the Identities / Certificate Configuration [185] field.

When "Certificate" is selected, Client and VPN gateway mutually authenticate each other using the certificates stored at Client and VPN gateway:
Client → VPN gateway using the Client's User Certificate and
VPN gateway → Client using the VPN gateway's Server Certificate.

Pre-shared Key

Enter the appropriate PSK in the Identities / Pre-shared Key [184] field.

When Pre-shared Key is selected, Client and VPN gateway mutually authenticate each other using the key preshared at both Client and VPN gateway - Client -> VPN gateway and VPN gateway -> Client.

EAP

Extended Authentication Protocol uses the username and password (VPN User ID and VPN Password) from the associated profile.

User ID and Password are configured in the Identities [183] field to authenticate the Client with the VPN gateway.

When EAP is selected, EAP is only used to authenticate the Client with the VPN gateway. The VPN gateway will use it's PKI Issuer Certificate to authenticate itself with the Client. To enable this VPN Server to Client authentication, the Server's CA certificate must be loaded at the VPN gateway and a Client User Certificate, from the same CA/Issuer.

It is loaded at the Client via the Identities / Certificate Configuration [185] field.

IKEv2 Policy [IPsec Configuration]

The parameters in this folder apply to phase 1 of the IKEv2 (Internet Key Exchange version 2) protocol with which the control channel for the security association (SA) is established.

The IKEv2 policies which you configure here will then be listed for selection in the "IKEv2 Policy" pulldown in the IPsec General Settings folder.

No IKEv2 policies are delivered with the software.

Algorithms and Parameters

Name [173 IKEv2 Policy] 173
Encryption [IKEv2 Policy] 173
Pseudorandom 173 Function [IKEv2 Policy] 173
Integrity Algorithm [IKEv2 Policy] 174

All the above parameters can be edited by selecting/adding the appropriate policy and modifying/adding the appropriate proposal.

Name [IKEv2 Policy]

When adding a new policy, first give it a name by which it can be referenced later.

Encryption [IKEv2 Policy]

Symmetrical encryption of IKEv2 messages 3 and 4 (the second exchange) in the Control Channel occurs according to the encryption algorithms negotiated beteween initiator and responder during messages 1 and 2 of the IKEv2 exchange (the first exchange).

The keys used are generated using the Pseudorandom Function negotiated between the two parties during the first exchange. In automatic mode the encryption is determined by the communication partner.

For each separate proposal select an Encryption algorithm from the pulldown list.

Pseudorandom Function [IKEv2 Policy]

Random values used for Integrity Protection and Encryption during the second IKE exchange are generated using a Pseudorandom Function negotiated between initiator and responder during the first exchange.

For each separate proposal select a Pseudorandom Function from the pulldown list.

Integrity Algorithm [IKEv2 Policy]

IKEv2 incorporates integrity protection functionality to protect the SA creation process from interference by third parties.

The cryptographic algorithm to be used for integrity protection is negotiated during the first IKEv2 exchange.

For each separate proposal select an Integrity Algorithm from the pulldown list.

IPsec Policy [Selection]

Preconfigured: ESP-AES128-MD5.

All IPsec policies which were created during software installation or during IPsec configuration are listed by name in the listbox.

automatic Mode:

In this case it is not necessary to configure the IPsec policy in the IPsec menu.

ESP-AES128-MD5:

If this IPsec policy is chosen, the same policy including its proposals must apply to all users, meaning that on both the client and the server the same proposals for the policies must be available.

If the Secure Entry Client is to use special policy proposals or lifetimes, use the [Policy Editor] and [Policy Lifetimes] buttons to create, modify or delete the respective details (see IPsec 162 Policy [Profiles]).

IPsec Policy [Profiles]

The parameters in this folder apply to phase 2 of the SA negotiation. The IPsec policies which you configure here are listed for selection for the internally created SPD.

Only one IPsec policy with ESP (Encapsulating Security Payload) is delivered with the software - ESP-AES128-MD5. As IPsec mode with AH security is unsuitable for flexible remote access, the AH protocol is not available.

Every IPsec policy lists at least one proposal for IPsec protocol and authentication, i.e. a policy can consist of one or more different proposals.

The same policies including the associated proposals should apply for all users. This means the same proposals should be available for the policies, both on the client side and on the central system.

Algorithms and Parameters

Name [IPsec Policy] 177
Protocol [IPsec Policy] 177
Encryption [IPsec Policy] 177
Authentication [IPsec Policy] 177

Name [IPsec Policy]

When adding a policy first give it a name by which it can be referenced later.

Protocol [IPsec Policy]

The default value is ESP.

Transform / Encryption

When using the security protocol ESP, the algorithm to be used for encrypting the payload can be selected from the displayed list.

Authentication [IPsec Policy]

Select the authentication mode to be used for the ESP security protocol from the displayed list.

PFS / DH Group

The selection of one of the available Diffie Hellman groups determines that a complete key exchange (PFS) should additionally occur in phase 2 with the SA negotiation. The higher the DH group, the more secure the Key Exchange.

IPsec Settings [Policies]

The IPsec policies are globally determined using this configuration window. In the "IPsec Settings" of the profile configuration they can be selected by needs.

Policy Lifetime [IPsec General Settings]

All IKE and IPsec policies are subject to the same set of lifetime parameters. These can be reconfigured if necessary and are accessed via the [Policy Lifetimes] button.

See also following topics:

Life 179 Type [Policy] 179
Dura 179 tion [Policy] 179
kBytes [Policy] 179

FIPS Certification

The IPsec Client incorporates cryptographic algorithms conformant to the FIPS standard. The embedded cryptographic module incorporating these algorithms has been validated as conformant to FIPS 140-2 (certificate #1747).

FIPS conformance will always be maintained when the following algorithms are used for establishment and encryption of the IPsec connection:

• Diffie Hellman Group: Group 2 to 14 (DH length of 1024 bits up to 2048 bits)
• Hash Algorithms: SHA1, SHA 256, SHA 384, or SHA 512 Bit
• Encryption Algorithms: AES with 128, 192 or 256 Bit or Triple DES

See also following topics:

IKE Policy [Selection] 168
IPsec Policy [Selection] 175

Lifetime Type [Policy]

Determines the criteria for key lifetime; this can be based either on duration or transferred bytes or both. When the counter (time or number of bytes) expires, a new SA negotiation takes place.

Lifetime [Policy]

Set the length of the life time for use of the policy. When the counter (time) expires, a new SA negotiation takes place. (Default Phase 1: 8 h, phase 2: 1 h.)

Volume [Policy]

The amount of kbytes specified here, which are transferred between client and server, determines the validity period of a security association (see IPsec Policy 162). After transmission of the specified kBytes, a new SA negotiation takes place. With each new SA negotiation, the counter is reset.

Advanced IPsec Options

Please also refer to the following topics:

IPsec Compression

Turn IPsec compression on or off using this switch. The remote station specifies which IPsec compression is used. The data transmission with IPsec can be compressed in the same way as with a transfer without IPsec. This allows for a maximum three-fold increase of the throughput.

Standard IPsec / UDP Encapsulation

Standard IPsec (port 500) or UDP encapsulation can be used.

When using UDP encapsulation, only port 4500 must be activated on the external Firewall (which is different with NAT Traversal or UDP 500 with ESP). If UDP encapsulation is used, then the port can be freely chosen.

 Port 4500 is set as default for IPsec with UDP; Port 500 for IPsec without UDP.

The NCP Gateway detects UDP encapsulation automatically.

Disable DPD (Dead Peer Detection)

DPD (Dead Peer Detection) runs in the background, when supported by the destination gateway. The IPsec Client uses DPD to check, at regular intervals, if the remote peer is still active.

When no data is received over the VPN tunnel, the VPN client will trigger DPD. If the VPN client receives a response from the VPN gateway, it will try again in the configured DPD interval.

If the VPN client does not receive a response, it will send a retry within 5 seconds to detect a dead session fast.

If the VPN client will receive no response after the amount of configured retries in a row, it will disconnect the session.

This functions switches off DPD.

Anti-replay Protection

The delayed arrival of IP packets could imply that these are damaged; if this function (based on RFC 2406) is enabled, such packets are discarded.

The following message shows that packages are recognized and dropped:

Esp: Warning - AntiReplay error on sequence number=xxxx

Enable negotiation according to RFC 7427

The client supports certificate authentication according to RFC 7427 for IKEv2 RSASSA-PSS which also allows for modern padding (RSASSA-PSS).

Default: enabled

VPN Path Finder

The major prerequisite for VPN Path Finder is a VPN gateway with VPN Path Finder technology (e.g. NCP Secure Server 8.00 or later). There, an alternative port must be configured in the VPN / IPsec settings of the local system.

Whenever a standard IPsec connection, i.e. via port 500 or UDP encapsulation via a freely configurable port, can not be established, VPN Path Finder automatically switches to the alternative connection protocol, TCP encapsulation with SSL Header (Port 443).

This is relevant when only HTTPS port 443 is available for the client and a standard IPsec connection can not be established. This is often the case, for example, in a hotel or at a hotspot.

If a proxy server is to be used for this connection, it can be set and configured in the configuration menu under Proxy for VPN Path Finder.

If a connection is established using this technology (i.e. using port 443), the monitor displays this via an icon in its state display (below and to the right of the HQ / gateway).

The monitor interface displays the icon after VPN dial up.

RFC 7427 padding method

If certificate-based authentication is activated for IKEv2 according to RFC7427, the desired padding method can be selected via this parameter.

The following padding methods are available:

• PKCS#1 v.1.5 Padding
• RSASSA-PSS

The default is: RSASSA-PSS

Note: The authentication for IKEv2 configured here, including the padding method, must be supported and accepted by the remote site.

IKEv2 RSA Authentication with PRF-Hash

The IKEv2 RSA Authentication parameter with the PRF hash means that the hash algorithm for IKEv2 RSA authentication does not use the standard recommended by RFC (SHA-1).

Instead, enabling this function causes the algorithm currently configured by the pseudorandom function 173 (PRF) from the IKEv2 policies to be used.

By default, this feature is disabled.

Identities

A number of more detailed security settings can be made that are dependent on the IPsec security mode.

See following parameters:

IKE ID-Type [Identity]

Native IPsec differentiates between outgoing and incoming connections. The value selected by the initiator as ID for an outgoing connection must be selected by the remote gateway as ID for incoming connections.

The following ID types can be selected:

• IP Address
• Fully Qualified Domain Name / (equivalent of host name)
• Fully Qualified Username / (e-mail address of the user)
• ASN1 Distinguished Name
• IP Subnet Address
• ASN1 Group Name
• Free String used to identify Groups

IKE ID [Identity]

For IPsec there is a differentiation of incoming and outgoing connections. The value selected by the IPsec initiator as ID for outgoing connections must also be selected at the remote gateway as ID for incoming connections.

Automatically Setting the VPN User ID

The administrator can centrally predefine an environment variable for the VPN User ID: %USERNAME% or % NCPUSERNAME% This variable is then read from the Secure Client PC and then used automatically for the VPN User ID.

If %USERNAME% is predefined, this Windows environment variable will be read once when the Secure Client starts for the first time after being installed and remains in effect for all subsequent system restarts.

If %NCPUSERNAME% is predefined, this Windows environment variable will be read each time the Secure Client starts, meaning that, after each Windows logon for a different user, the current USERNAME is read from the Windows settings.

These variables cannot be used when Windows logon is via the credential provider.

Enter the IKE ID-Type 184 string that corresponds to the associated "IKE ID Type".

The default for the type is U-FQDN (Fully Qualified Username)

Pre-shared Key

"IPsec Pre-shared Key" is the password required to build a tunnel to the VPN gateway. The tunnel is only set up if the password set in the VPN Gateway is the same as the password set at the Secure Client. The "IPsec Pre-shared Key" can be up to 16 characters long.

Certificate Configuration [Profiles]

A certificate which was installed using the client monitor's Certificate Configuration can be selected here for extended authentication (XAUTH).

none:

A certificate is not used for data encryption and authentication.

Standard PKI configuration:

The certificate configuration of a client older than version 9.1 will, in the case of an update to this version, be automatically converted to the default PKI configuration. The default PKI configuration is also set up after a first installation of version 9.1 if a test connection with certificate is established.

Extended Authentication (XAUTH)

On the Entry Client, extended authentication (XAUTH protocol, draft 6) is not active by default. It can be switched on at this point if it is supported by the IPsec gateway. In addition to the pre-shared key, the following parameters can also be used for authentication:

User ID [Identity]

Obtain the user ID for XAUTH from your system administrator. The name may be up to 256 characters long.

Password [Identity]

Obtain the password for XAUTH from your system administrator. The name may be up to 256 characters long.

Alternatively a certificate of the certificate configuration can be used.

If the Internet Key Exchange protocol version 2 (IKEv2) is selected, the Microsoft CHAP version 2 (MSCHAPv2) authentication protocol is used.

User ID [Identities]

Contact your System Administrator for your "User ID". The name can be up to 256 characters long.

Note: This parameter pertains only to accessing the gateway at the remote site.

Password [Identities]

Contact your System Administrator for your "Password" for XAUTH. The password can be up to 256 characters long.

Note: This parameter pertains only to accessing the gateway at the remote side.

Access Data from the Configuration

You can select one of the following methods for authenticating the VPN tunnel against the gateway:

Access data from the configuration above

The VPN tunnel will be authenticated based on the User ID and Password entered in the respective fields above.

Access data from certificate's field e-mail

The VPN tunnel will be authenticated based on the contents of e-mail field of the selected certificate.

Access data from certificate's field (common name)

The VPN tunnel will be authenticated based on the contents of the "Subject" field of the selected certificate.

Access data from certificate's field serial no.

The VPN tunnel will be authenticated based on the contents of "Serial No." field of the selected certificate.

Access data from certificate's field (User Principal Name, UPN)

The VPN tunnel will be authenticated based on the "User Principal Name" (Loginname@Domain-Name), assuming the attribute is present in the certificate.

Access data from certificate's field (Subject Alternative Name: E-Mail)

The VPN tunnel will be authenticated based on the display-name of the e-mail address.

IPsec Address Assignment

When using native IPsec, the Client's IP addresses can be assigned in in a number of different ways, each of which can be configured here.

Note:

Assignment of the Private IP Address

Use this parameter to define how the IP address should be assigned. Select the option required from the pulldown list.

IKE Config Mode

With IKE config mode (Draft 2) the IP addresses of the client, the DNS servers as well as the domain name are dynamically assigned.

All previous WAN interfaces can be used for the NAS dial-up.

With IPsec tunneling, DPD (Dead Peer Detection) and NAT-T (NAT Traversal) are automatically executed in the background, when this is supported by the remote gateway. The client uses DPD to check, at pre-specified intervals, whether the remote gateway is still active. If the remote gateways fails to respond then the connection is automatically disconnected.

The negotiation of NAT Traversal is handled automatically by the client and is always necessary when a device using network address translation is employed by the destination system.

Local IP address

In this case the IP addresses (also DHCP) currently configured in the computer's network settings are used for the IPsec Client.

This is the default setting for the Entry Client.

Manual IP address

Enter the IP address and the subnet address here. In this case the addresses entered here are used, independently of the configuration in the computer's network settings.

DHCP over IPsec

As an alternative to using IKE config mode, a DHCP server of the gateway can also be used; the IP address is then assigned to the client via the VPN tunnel by means of a DHCP negotiation.

One or two DNS servers can be assigned, dependent on your requirements; the primary server is used as the default server.

DNS / WINS Server

You can define an alternative DNS server as opposed to using the one that is automatically assigned during the PPP negotiation. Please be sure to activate "Enable DNS" in the DNS configuration folder under the windows network settings.

In accordance with your requirements you can assign one or two DNS servers. The primary server is used as the default server. If no alternative server has been defined, the server assigned via PPP is used.

First / Second DNS Server: The first DNS server entry is used instead of the address assigned during any connection establishment negotiations. The second DNS server entry is used as a backup server.

Domain Name

This Domain Name replaces the domain name which would normally be updated in the computer's network settings using DHCP.

E.g.: Host Name.Domain Name (Computer1.Company.3rdFloor.at)

DNS domains to be resolved in the tunnel

Enter the domain names here that are to be resolved on the client side on the NCP virtual adapter.

Split Tunneling

Exactly those IP networks can be defined here, with which the client must communicate via VPN tunnel. If tunneling is used and no entries are made here, then the connection will always be established to the tunnel endpoint of the gateway. Should both tunneling to the central office and communication via the Internet be enabled simultaneously, then enter in this list the IP network(s) that the client may only reach via the tunnel. You will then be able to alternate between access to the Internet and the gateway of the company headquarters. This is known as Split Tunneling.

Click on the "Add" button and enter IP address and network subnet mask in the window which appears.

Please also refer to:

Remote IP Networks (IPv4) 190

Full Local Network Enclosure Mode 191

Remote IP Networks (IPv6) 191

Remote IP Networks (IPv4)

Enter here the address of the IP network to be reached by the client via the VPN Gateway. You can obtain the address(es) from your system administrator.

If you do not make an entry in this list, all IP packets will be sent via the VPN tunnel.

Please make sure that the IP address of the VPN Gateway does not lie in the range of the network addresses.

A maximum of twenty networks can be configured.

Remote IP Net Masks

Enter the appropriate IP network subnet mask here. You obtain the address(es) from your system administrator.

Please make sure that the IP address of the VPN Gateway does not lie in the range of the network addresses.

In the case of Split Tunneling refer to the notes about DNS queries under DNS domains to be resolved in the tunnel.

Alternative address input

If the prefix length is additionally entered when entering the IP address (for example, 175.16.15.0/24), the subnet mask is created from the prefix length when leaving the input field and entered in the corresponding column.

Full Local Network Enclosure Mode

Enable this function if you wish to route all the local LAN traffic over the VPN tunnel.

Remote IP Networks (IPv6)

Data entry for an IPv6 network is accomplished by entering the IP address and attached prefix length (e.g., `2001: 0db8: 85a3: 08d3 :: / 64`).

A maximum of twenty networks can be configured.

VPN bypass

The application or domain can be selected from the VPN bypass list that should bypass the VPN while the currently selected VPN profile is active.

Please note that any firewall rules configured in the Client do not apply for these applications and domains. Bypass traffic cannot be restricted by firewall rules and is not logged by the client firewall.

(Refer to VPN-Bypass-Function 204)

Certificate Check

Checking the certificate contents

You can specify in the "Certificate Check" parameter field, per destination system, which entries must be present in a certificate from the remote side (Secure Server)(see: Display Incoming Certificate, General).

Please also refer to the following topics:

Incoming Certificate's Subject

All attributes of the user, to the extent known - even with wildcards -, can be used as user certificate entries of the remote side (server). In this regard compare the entries that are always listed under users for "Display Incoming Certificates".

Use the attribute name abbreviations for this. The attribute type abbreviations for certificate entries are as follows:

cn	Common Name
s	Surname
g	Givenname
t	Title
o	Organization
ou	Organization Unit
c	Country
st	State
l	Location
email	e-mail
sn	Serialnumber

Example:

cn=VPNGW*, o=MyCompany, c=de

In the above example:

- The common name of the security server is checked here only as far as the wildcard "*". All subsequent positions, such as 1 - 5 as numbering, will be ignored.

- The organization must always be "MyCompany".

- The country must be United States.

Incoming Certificate's Issuer

All attributes of the user, to the extent known - even with wildcards -, can be used as user certificate entries of the other side (server). In this regard compare the entries that are always listed under users for "Display Incoming Certificates".

Use the attribute name abbreviations for this. The attribute type abbreviations for certificate entries have the following meaning:

cn	Common Name
s	Surname
g	Givenname
t	Title
o	Organization
ou	Organization Unit
c	Country
st	State
l	Location
email	e-mail
sn	Serialnumber

Example:

cn=My Common Name

Only the common name of the issuer is verified here.

Issuer's Certificate Fingerprint

In order to prevent an unauthorized person, imitating a trusted CA, from using a counterfeited issuer certificate, the issuer's fingerprint can also be entered if it is known.

A comparison check is performed on each character entered, and each character must exactly match the corresponding character in the fingerprint, starting from the first, i.e. left most character. The accuracy of the check increases with the number of characters entered.

SHA1 Fingerprint

The algorithm for fingerprint generation can be either MD5 (Message Digest version 5) or SHA1 (Secure Hash Algorithm 1).

Further Certificate Checks

In addition to the certificate verification according to content a certificate check is executed on the Secure Client in many respects.

1. Selection of the CA Certificates

The corporate network administrator specifies which issuers of certificates can be trusted. This is done by copying the CA certificates of his choice into the %INSTALLDIR%\CACERTS\ directory.

The formats *.pem and *.crt are supported for issuer certificates. They can be viewed in the monitor under the menu item "Connection / Certificates / Display CA Certificates".

If the issuer certificate of another side is received, the client determines the issuer, searches for the issuer certificate, first on smartcard or in the PKCS#12 file, and then in the %INSTALLDIR%\CACERTS\ directory. If the issuer certificate cannot be located, then the connection cannot be established.

If no issuer certificates are present, no connection is permitted.

2. Check of Certificate Extensions

Certificates can contain extensions. These serve for the linking of additional attributes with users or public keys, that are required for the administration and operation of the certification hierarchy and the revocation lists. In principle, certificates can contain any number of extensions, including those that are privately defined. The certificate extensions are written in the certificate by the issuing certification authority.

Three extensions are significant for the Secure Client and the Secure Server:

• extendedKeyUsage
• subjectKeyIdentifier
• authorityKeyIdentifier

extendedKeyUsage:

If the extendedKeyUsage extension is present in an incoming user certificate, the Secure Client checks whether the defined extended application intent is "SSL Server Authentication". If the incoming certificate is not intended for server authentication, the connection is refused. If this extension is not present in the certificate, this will be ignored.

Please note that the SSL server authentication is direction dependent. This means that the initiator of the tunnel establishment checks the incoming certificate of the other side, if the extendedKeyUsage extension is present, then the intended purpose must contain "SSL Server Authentication".

subjectKeyIdentifier / authorityKeyIdentifier:

A key identifier is an additional ID (hash value) to the CA name on a certificate. The authoritykeyidentifier (SHA1 hash over the issuer's public key) on the incoming certificate must agree with the subjectKeyIdentifier (SHA1 hash over the public key of the owner) on the corresponding CA certificate. If no CA certificate is found then the connection is rejected.

The keyidentifier designates the public key of the certification authority and thus not only one, but a series of certificates if required. The use of the key identifier allows a greater flexibility for the determination of

a certificate path. In addition, the certificates that possess the authoritykeyidentifier extension do not need to be revoked if the CA issues a new certificate when the key remains the same.

3. Checking Revocation Lists

The Secure Server can be provided with the associated CRL (Certificate Revocation List) for each issuer certificate. It will be copied into the %INSTALLDIR%\crls\ directory. If a CRL is present, then the Secure Client checks the incoming certificates to see if they are listed in the CRL. The same applies to an ARL (Authority Revocation List) that must be copied into the %INSTALLDIR%\arls\ directory.

If incoming certificates are contained in the CRL or ARL lists, then the connection is not permitted.

If CRLs or ARLs are not present, then no check takes place in this regard.

Link Firewall

The settings of the Link Firewall can also be used for RAS connections. If the Link Firewall has been enabled, a shield icon with arrows is displayed in the graphic filed of the monitor.

A firewall's fundamental task is to prevent viruses etc. from other networks or the Internet from spreading within the corporate network. This is why a firewall is also installed at the junction between a corporate network and the Internet. It checks, based on previously defined conditions or rules, all incoming and outgoing data packets and decides whether or not a data packet can be allowed through the firewall.

The Link Firewall uses stateful inspection technology. Security is ensured from two perspectives: stateful inspection functionality prevents unauthorized access to data and resources in the central data network and as a "door-keeper" it monitors the status of all existing Internet connections. In addition, the stateful inspection firewall recognizes whether a connection has opened "spawned connections" - such as with FTP or Netmeeting - whose packets likewise must be forwarded. The Stateful Inspection connection represents a component of the direct line to the communication partner, a component that may only be used for exchanging data that conforms to one of the agreed-upon rules.

Please also refer to the following topics:

Stateful 198 Inspection 198
Only Tunneling 198 Permitted 198
In Combination with Microsoft's RAS Dialer only Tunneling Permitted 198

Stateful Inspection

off: The Link Firewall's security mechanisms are not used.

always: The Link Firewall's security mechanisms are always used, this means the PC is protected from unauthorized accesses even if no connection is established.

when connected: The device is not vulnerable if a connection exists.

Only Tunneling Permitted

Only communication within the tunnel permitted: if the Link Firewall has been enabled, this function can also be switched on, ensuring that only incoming or outgoing VPN connections are allowed. All other data traffic will be rejected.

In Combination with Microsoft's RAS Dialer

When using the Client Monitor this function prevents communication to the Internet via the RAS Dialer.

Compressed connections of the RAS Dialer can also be monitored by the client, in addition to normal IP traffic. This is the case, because CCP and VanJacobson IP Header (in IPCP) are no longer negotiated.

Features

The following sections describe the configuration and use of specific functions via the menu in the client interface:

Home Zone

The Function of the Home Zone

If a user is working on the corporate network, they can use all the resources that are permitted by access rights and firewall settings.

The remote user can also access these resources from home via VPN (or SSL VPN) and work on their computer as if connected to the company network. Some devices, however, such as a printer or special applications (own database, FTP or Web server) which are located on their home network are not available.

The Home Zone feature has been implemented as an option in the firewall so that the user can still access resources on their home network without the administrator having to know about each IP network in their employee's home office.

Similarly, the Home Zone feature can be used for various other tasks, for example, to enable service technicians to work on machine control systems if the machines are connected via TCP / IP to the network that the technician is connecting from and this network should neither be a known network with completely transparent communication or an unknown network with completely restrictive communication and the IP address range cannot be added as exceptions in the firewall, as it may not be known in advance.

If a user's computer is located in a Home Zone and the Client on this computer is used to establish a VPN connection to a company network, the company's policies will apply.

Client Configuration:
• This requires that Home Zone is activated under "General" in the firewall options 71 . For connecting to the private network LAN or Wi-Fi is to be used in the background.
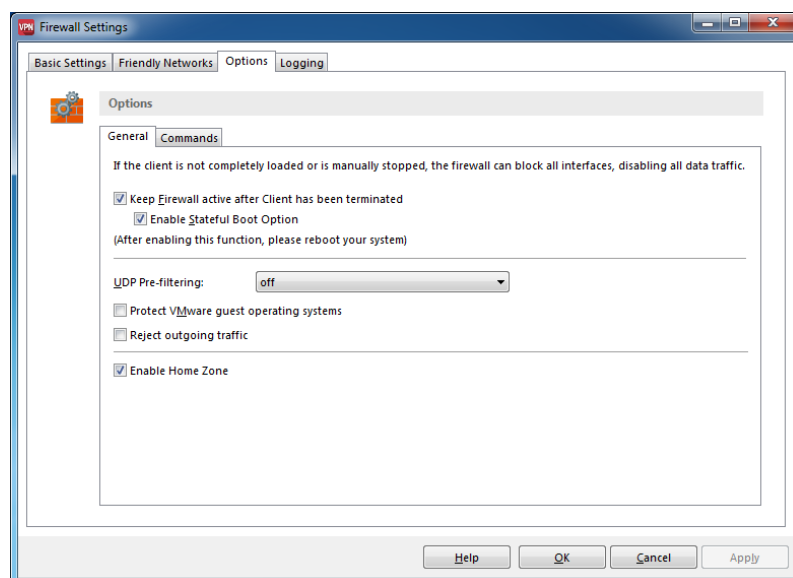
Other interfaces, such as mobile broadband or dial-up cannot be used for a Home Zone. The MAC address of the default gateway of the active network adapter is set as the Home Zone. This means that the administrator does not require knowledge of the private network.

• The default firewall rule "Home Zone" under "Firewall / Preferences" 54 must also be added to the active firewall and be enabled. If the administrator wants to restrict a firewall rule so that it only applies for local IP networks connected to the end device, the new "anylocalzone" variable can be used in addition to "anyv4" and "anyv6".
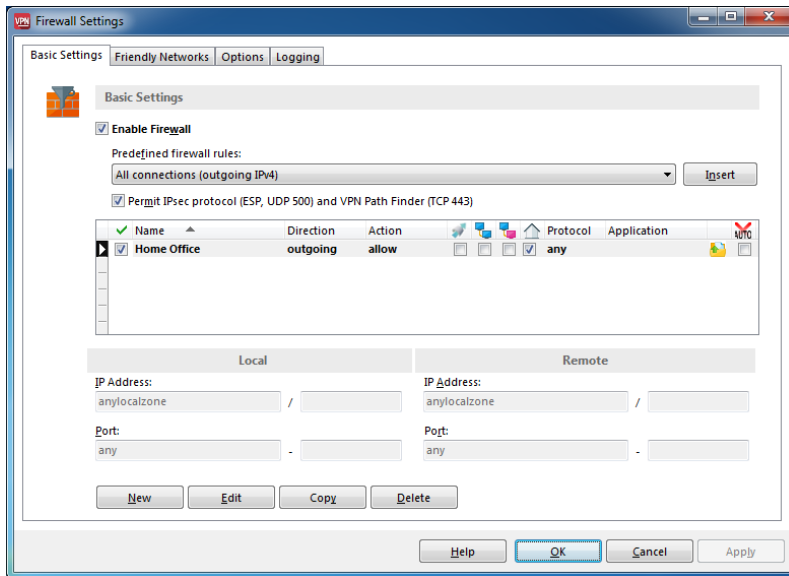
As the administrator does not usually know the IP address of the private network, the default IP address range is set to "anyLocalZone". For local and remote ports "any" is set by default which gives the user complete access to the Home Zone, i.e. their own network. Optionally, the IP address ranges and the permitted ports can be modified.

• Automated actions can be executed once the firewall rule for the Home Zone is activated in the client, exactly the same as for known networks or unknown networks. This can be configured in the client configuration menu under "Firewall / Friendly Networks / Actions" | 66 |.

If these settings have been made, "Home Zone" | 26 | is displayed in the connect menu of the GUI.

Using the Home Zone Feature via Client GUI

The user can now set or delete the Home Zone | 26 | with a single click. When the Home Zone is configured and active, it is displayed in the client monitors GUI with the symbol of a house on the desktop behind the protection shield of the active firewall. (Fig. below)

By setting the Home Zone,
the Home Zone rule is activated and the MAC address of the default gateway of the active network adapter is stored in the client's configuration. If multiple network interfaces are active and each has a default gateway, the default route that has the smallest metric is considered for saving the MAC address.

If another private network is used as a Home Zone at a later date, the user can click on "Set" when they are connected to the new private network. The MAC address set for each Home Zone is displayed in the Client Info Center | 124 |. The previous MAC address is overwritten each time the Home Zone is set.

With these settings, it is possible for the user to access all resources in their private network.

By deleting the Home Zone,
the Home Zone can be removed or disabled again, for example also when this function has been activated by accident (the status is shown by the house symbol. The Home Zone can only be deleted correctly when the network adapter is in the Home Zone (and if applicable an external adapter is connected) and if the system is rebooted after the Home Zone is deleted.

When the user logs in to the corporate network again at work via LAN or Wi-Fi after working in the Home Zone in their home office is automatically no longer connected to the Home Zone in their private network. Access to the resources on the corporate network will be controlled again through access permissions and firewall settings (if applicable through Friendly Net Detection).

If the user connects to the network, in which they have previously set the Home Zone after some time, but has not currently set or deleted the Home Zone, the Client recognizes the network based on the hardware address of the router and activates the Home Zone firewall rule on the network interface which the router is connected to. If another network interface is active with a default gateway that has a different MAC address, the Home Zone firewall rule will not be active on this interface.

In the Monitor Log of the Client
Home Zone connections are logged as follows:
... enter home-zone
… exit home-zone

(See Help / Logbook 121)

VPN bypass

The VPN bypass function

The VPN bypass function allows the administrator to define applications or domains which can communicate over the Internet directly despite disabling Split Tunneling [190] on the VPN connection.

This function can be used to separate non-sensitive data traffic from the central infrastructure, so as not to affect performance. For example, operating systems and virus scanner updates (with a known domain), can bypass the VPN connection easily, or certain cloud services direct can per permitted direct access to applications via the Internet.

Client Configuration
The applications and domains for the VPN bypass function can be configured by the corporate network administrator or by the user directly in the client.

• Firstly the applications or domains which need to bypass the VPN tunnel are defined in the configuration menu of the client GUI under "VPN bypass [75]". It can be defined whether the VPN bypass function should apply to TCP or UDP traffic.

This list of applications and domains which should bypass the VPN are needed for additional configuration.

• In the client VPN profiles of clients which can be accessed from the configuration menu of the GUI under "Profile", the application or domain can be selected from the VPN bypass list [191] that should bypass the VPN while the currently selected VPN profile is active.

- In addition to the name for the VPN bypass list, you can also specify the IP addresses for a primary and secondary DNS server.

- The DNS entry for VPN bypass ensures that for external VPN bypass destinations, name resolution through the VPN tunnel is performed only by the two configured DNS servers. For this purpose, a primary and a secondary DNS, optionally as IPv4 or IPv6 address, can be entered in the VPN bypass configuration.

> **Note:** The configured DNS servers are only effective for configured web domains. Configured applications within the VPN bypass functionality are not taken into account.

Please note that any firewall rules configured in the Client do not apply for these applications and domains. Bypass traffic cannot be restricted by firewall rules and is not logged by the client firewall.

Biometric Authentication

The functionality of biometric authentication via "Windows Hello" before VPN connection establishment is available from version 11.1 on.

As of Client version 11.1, user authentication can be required before any manual VPN connection is established. This feature provides enhanced protection against unauthorized third party access to an unlocked workstation. It prevents unauthorized VPN connections to the central company network. Windows 8.1 or Windows 10 and the Windows Hello login option are required to use this feature.

Windows Hello must be configured accordingly so that a user can log on to their local computer. Windows Hello must be configured after setting up the biometric device with fingerprint or face recognition data. Depending on authentication method priority and the available devices, users can also enter their user name and password for authentication.

Configuration

The client software can also enforce the local authentication procedure before initiating the VPN connection and request the same authentication data that the user uses to log onto the Windows system. To do this, configure the following in the client VPN profile: Enable the option "Fingerprint reader / biometric authentication" under "Advanced authentication"

When this setting is enabled, an authentication prompt is displayed as soon as the user clicks connect in the client. The VPN connection will only be initiated after successful authentication via the method configured for Windows Hello (fingerprint recognition, face recognition, PIN entry, etc.).

User interaction is required to use advanced authentication through Windows Hello and ensure a secure connection. For this reason, advanced authentication cannot be used using the "automatic" or "always on" connection modes. The connection mode in the VPN profile must be set to "manual" or "variable" to use this feature. This setting can be enable in the VPN profile under "Line Management / Connection Mode".

Procedure

The authentication prompt displayed by the operating system depends on the Windows version and the hardware configuration of the computer. If the computer does not have any hardware for biometric authentication, or if this is not activated, the dialog for entering user name and password appears, whereby the user name can no longer be entered, since this already took place when the user logged on to the local computer.

The authentication prompt contains texts from the operating system and the client, which is why different languages can appear in the dialog if the operating system and the client have different language settings.

Credential Provider

The Credential Provider initiates a VPN connection to the company network when the user logs on to Windows. This means that user authentication does not take place on the local Windows system, but on a Windows domain. However, using the Credential Provider excludes the use of biometric authentication before the VPN connection is initiated by the Client.

### Parameter and Configuration Locks

A configuration lock can be set by administrators for the Client so that this feature is not visible to the user under profile settings and can therefore no longer be configured.

Credential Provider

The Credential Provider is always automatically set up with the client software. On the desktop it looks like the client GUI.

Initialisation

The Credential Provider is initialized via the client interface: To do this, select "Logon Options" under the "Configuration" menu and activate the option "Display connection dialog before Windows logon" under the Logon 107 tab. (Fig. below)
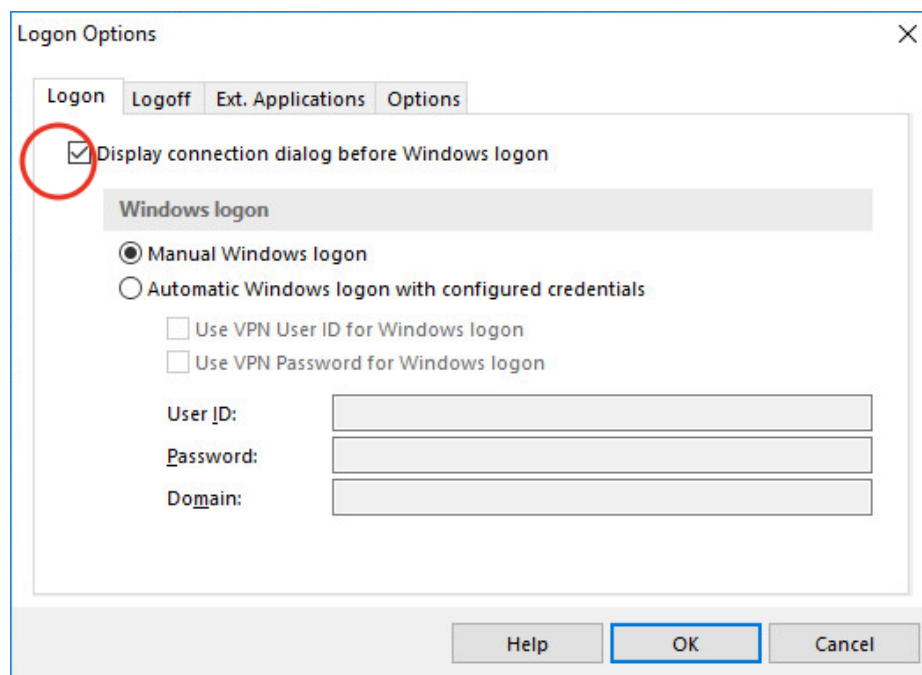
(Further configuration options are available under the Ext. Applications 109 and Options 110 tab after the above option has been enabled).

After logging off from the system or rebooting, the VPN icon for pre-logon (and the product name of the client) is displayed under the user logon icon on the Windows start screen. The VPN icon will then appear in green on the Windows start screen if pre-logon has already taken place.

Credential Provider Dialog

When pre-logon is enabled, the Credential Provider dialog is displayed and the user is prompted to establish the connection. The VPN connection for logging on to the Windows domain can now be established by clicking on "Connect". (Depending on the profile or certificate configuration, the user may be required to enter a PIN).

Client Monitor

After the user logs on to the domain, the client monitor is displayed. All client configuration options may be accessed via the client monitor.

Domain logon options can only be modified through the client monitor.

Pre-logon Features

In the configuration dialog of the Credential Provider, the functions and configuration options that are possible in the pre-logon stage can be executed.

In the "Connection" menu this includes manually connecting/closing the connection, retrieving statistical information and Hotspot Logon 26 .

Wi-Fi options 83 can be configured under the "Configuration" menu.

User Authentication with the Credential Provider

The Credential Provider initiates a VPN connection to the company network when the user logs on to Windows. This means that user authentication does not take place on the local Windows system, but on a Windows domain. Biometric authentication using Windows Hello before the VPN connection is established is not possible.

QoS (Description)

Quality of Service (QoS) is the quality of a communications service from the user's point of view. The quality of service is measured by how the service meets the appropriate requirements.

In networks, all data packets are usually treated equally, regardless of which applications. As long as the network only transmits data packets from applications that require low bandwidth, a fully utilized bandwidth can only be noticed by short delays during data transmission.

In use of real-time applications, which require a higher bandwidth, like Voice Over IP Telephony or video streaming (skype, youtube,...), delays and loss of data packages have a negative effect. In VoIP telephony this occurs by terminating, delayed calls or by a low voice quality, in video streaming through unsynchronized transmission of image and sound.

Responsible for this is the standard network protocol TCP / IP, which does not distinguish from which application which data was sent and transmits the data the same way. So when the bandwidth is utilized, all the data packets in the transmission are split evenly and the quality of the real-time applications decreases.

With the help of the "Quality of Service" (QoS) certain data packets can now be prioritized. It is important that the connected router, via which the IP telephony is transmitted, knows QoS. By prioritizing the data stream, real-time applications can be favored for bandwidth allocation, providing the bandwidth needed for a high-quality application with no crash or distortion. Other bandwidth-intensive applications must then wait until enough bandwidth is released.

QoS works as a "bandwidth management". It does not offer extra bandwidth, it priorizes selected data transmissions.

Clients in VPN

This function is added to the Client. With this function it is possible to determine a minimum bandwidth of the data traffic for a selected application or service. If there is a high network utilization VoIP packets can still be sent with a good sound quality.

To configure Quality of Service in the best way it is necessary to know the maximum available bandwidth. By specifying the bandwith choose your actual bandwith or a lower value. If your configured maximum is too low it can happen that the bandwidth won't be used productively. (There are no log-files for QoS).

VPN and Connection Direction

The prioritization of the packets takes place only for the traffic of the VPN connection, not over other LAN adapters.

QoS can only be used to send data from the client to the gateway. The receiving of data from the gateway is not regulated by QoS.

Available Bandwidth

When configuring QoS, a value for the maximum available network bandwidth must be configured. This value can be between 1 and 100 megabits per second and must be given in integers.

A VPN profile with a QoS configuration can not send more data than are configured even if more is available. The data rate will always be limited to the configured value. If configured too high, the actual data rates of the configured QoS groups will not match the expected results.

Fluctuating Bandwidths

In the case of varying bandwidths, such as Wifi or mobile communications, the configured minimum bandwidth of a QoS group can not be guaranteed. Although the configured bandwidth is reached on average, it may be temporarily lower.

QoS is also supported in Seamless Roaming, the automatic change of the connection medium. The maximum bandwidths for the various connection media (LAN, Wifi, mobile) are usually very different, so the corresponding QoS value can not be configured correctly.

Filter Types

A configured filter with the type "directory" does not consider applications in subdirectories. The configuration of the directory is "case sensitive".

The configuration for a application filter is "case sensitive".

It is not possible to include the file transfer of Windows Explorer in a QoS group. As "work around" one application can be configured as "unknown". It may happen that other applications, which are called in the VPN service as "unknown" are taken into account.

IPsec RFCs

RFCs implemented / used in Client Products

IPsec general

rfc4301- Security Architecture for the Internet Protocol

rfc4945 - The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX

IANA defined parameters and transform IDs

- IKEv1 - Internet Key Exchange (IKE) Attributes

- IKEv2 - Internet Key Exchange Version 2 (IKEv2) Parameters

- ISAKMP (ESP, ...) - "Magic Numbers" for ISAKMP Protocol

ESP

- rfc4303- IP Encapsulating Security Payload (ESP)

- rfc3948- UDP Encapsulation of IPsec ESP Packets

IKEv1

- rfc3526- More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)

- rfc3947- Negotiation of NAT-Traversal in the IKE

IKEv2

- rfc7296- Internet Key Exchange Protocol Version 2 (IKEv2)

- rfc4555- IKEv2 Mobility and Multihoming Protocol (MOBIKE)

- rfc5685- Redirect Mechanism for the Internet Key Exchange Protocol Version 2 (IKEv2)

- rfc5739- IPv6 Configuration in Internet Key Exchange Protocol Version 2 (IKEv2)

- rfc7383- Internet Key Exchange Protocol Version 2 (IKEv2) Message Fragmentation

- rfc7427- Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)

    - rfc3279, Section 2.2.3 - ECDSA Signature Algorithm (ECDSA)

    - rfc3447, Section 8 - RSASSA-PSS und RSASSA-PKCS1-v1_5 signature schemes

ECC

- rfc5639- Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation

ECC in DH

- rfc5903- Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2

- rfc6954- Using the Elliptic Curve Cryptography (ECC) Brainpool Curves for the Internet Key Exchange Protocol Version 2 (IKEv2)

- rfc6989- Additional Diffie-Hellman Tests for the Internet Key Exchange Protocol Version 2 (IKEv2)

Ecc in AUTH Payload

- rfc4754- IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)

Algorithms

CBC

- rfc2451- The ESP CBC-Mode Cipher Algorithms

AES-CTR

- rfc3686- Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)
- rfc5930- Using Advanced Encryption Standard Counter Mode (AES-CTR) with the Internet Key Exchange version 02 (IKEv2) Protocol

AES-GCM

- rfc4106- The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)
- rfc5282- Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol
- rfc6379- Suite B Cryptographic Suites for IPsec

Padding

- rfc3447, Section 8- RSASSA-PSS und RSASSA-PKCS1-v1_5 signature schemes

EAP

- IANE EAP Registry
- rfc3748- Extensible Authentication Protocol (EAP)

Utilities

There are applications in the client installation directory which can be controlled by batch or script files.

The command line tools must be started with the relevant commands and parameters from a command line window in the installation directory:

[Description of the commands, parameters and return values of NCPClientCMD.EXE](#) 214

The following advanced functions can be used with NCPRWSNT.EXE:

[Advanced Functions with NCPRWSNT.EXE](#) 228

Information about the General Registry Values can be found [here](#) 230.

Command Line Interface NCPClientCMD.EXE

NcpClientCmd /connect

This command initiates the connection establishment process without waiting for the process to complete.

Command: NcpClientCmd /connect [ProfileName] [user] [pwd]

Parameters:

ProfileName = name of the profile to use for the connection. If a profile name is not entered, the connection is established using the current profile (optional)

UserID = User name for VPN connection (optional)

Password = password for VPN connection (optional)

Return values:

0 = OK - connection establishment has been initiated

11 = error - system is already in a known network

12 = error - the profile name does not exist

13 = error - PIN for the certificate was not entered

14 = error- no authentication data for internet connection

15 = error - no authentication data available for VPN connection

Example:

NcpClientCmd /connect MyProfile user MyUserID pwd MyPassword

NcpClientCmd /connectWait

This command initiates the connection establishment process and remains active until the connection is established or the timeout expires (default value: 60 seconds).

Command:

NcpClientCmd /connectWait [Timeout]

Parameters:

Timeout = Maximum timeout for establishing a connection in seconds.

Return value:

0 = OK Connection established successfully

10 = error - timeout expired

11 = error - system is already in a known network

---

13 = error - PIN for the certificate was not entered

14 = error - no authentication data for internet connection

15 = error - no authentication data available for VPN connection

XX = error - specific error code

NcpClientCmd /disconnect

This command disconnects the connection without waiting for the connection to disconnect completely.

Command:

NcpClientCmd /disconnect

Parameters:

Return value:

0 = connection is being disconnected

NcpClientCmd /disconnectWait

This command disconnects the connection and waits until the connection has disconnected completely.

Command:

NcpClientCmd /disconnectWait

Parameters:

Return value:

0 = connection is being disconnected

16 = new configuration could not be read

146 = the NCPRWSNT service is not started

NcpClientCmd /getConnectState

This command returns the current connection status.

Command:

NcpClientCmd /getConnectState

Parameters:

Return value:

0 = Connection is disconnected

1 = Connection is being established

2 = Connection was successfully established

XX = Specific error code

20 = NCPRWSNT service didn't boot up

NcpClientCmd /getServiceState

The command returns the current status of the NCPRWSNT service.

Command:

NcpClientCmd /getServiceState [Time]

Parameters:

Time = maximum time (in seconds) to wait for the service to start

Return value:

0 = OK

20 = error - NCPRWSNT service is not started

21 = error - NCPRWSNT service did not answer

NcpClientCmd /select

This command switches the active profile.

Command:

NcpClientCmd /select

Parameters:

ProfileName = profile to be switched to

Return value:

0 = OK - the active profile was switched successfully

1 = error - incorrect parameter

12 = error - profile name entered does not exist

Example:

NcpClientCmd /select "Test connection IPsec IKEv1"

NcpClientCmd /sleep

This function can be used to set a waiting time between commands in a batch file.

Command:

NcpClientCmd /sleep

Parameters:

Time = waiting time in milliseconds

Return value:

0 = OK

NcpClientCmd /stop

This command stops all Client applications and services.

Command:

NcpClientCmd /stop

Parameters:

Return value:

0 = OK

NcpClientCmd /start

This command starts all Client applications and services.

Command:

NcpClientCmd /start

Parameters:

Return value:

0 = OK

NcpClientCmd /setInitUser

If the client should be personalized without user intervention, authentication data can be added with this command.

Command:

NcpClientCmd /setinituser [Password]

Parameters:

InitUserId = username for personalization

Password = password for personalization (optional)

Return value:

0 = OK

1 = error

NcpClientCmd /rsuAutoAnswer

This command specifies whether user interaction is required during the configuration update.

Command:

NcpClientCmd /rsuAutoAnswer

Options:

- Off = user interaction

- Yes = accept configuration without user interaction

- No = reject configuration without user interaction

Return value:

0 = OK - option configured

1 = error - option could not be configured

Example:

NcpClientCmd /rsuAutoAnswer off

NcpClientCmd /ginaInstall

This command installs the Credential Provider and returns the installation status.

Command:

NcpClientCmd /ginaInstall

Parameters:

Return value:

0 = OK - installation successful

1 = error - installation failed

NcpClientCmd /ginaUninst

This command deinstalls the Credential Provider and returns the installation status.

Command:

NcpClientCmd /ginaUninst

Parameters:

Return value:

0 = OK - deinstallation successful

1 = error - deinstallation failed

NcpClientCmd /ginaOn

This command activates and displays the Credential Provider during Windows Logon.

The Credential Provider must already be installed. If the Credential Provider was not installed during the installation, use the command "ncpClientCmd [[/ginaInstall]]" to install it.

Command:

NcpClientCmd /ginaOn

Parameters:

Return value:

0 = OK - activation successful

1 = error - activation failed

NcpClientCmd /ginaOff

This command deactivates and hides the Credential Provider during Windows Logon.

Note that this command does not remove the Credential Provider, it is only hidden. To deinstall the Credential Provider use the command "ncpClientCmd [[/ginaUninst]]"

Command:

NcpClientCmd /ginaOff

Parameters:

Return value:

0 = OK - deactivation successful

1 = error - deactivation failed

NcpClientCmd /ginaInfo

The command indicates whether the Credential Provider is installed.

Command:

NcpClientCmd /ginaInfo

Parameters:

Return value:

0 = not installed

1 = installed

NcpClientCmd /writeReaderIni

This command writes the "reader.ini" file in the given directory. The "reader.ini" is required by the SEM for displaying details of chip-card readers connected to local systems.

Command:

NcpClientCmd /writeReaderIni

Parameters:

OutputPath = directory where "reader.ini" is to be written (without a filename)

Return value:

0 = OK - the "reader.ini" was written successfully

1 = error - incorrect parameter

10 = error - the "reader.ini" file could not be written

NcpClientCmd /writeClientInfoCenterData

This command outputs the information from the "Client Info Center" and creates a file "ClientInfoCenter.txt". If a directory path is not entered, the file is written to the user's document directory.

Command:

NcpClientCmd /writeClientInfoCenterData [OutputPath]

Parameters:

OutputPath = directory path for the "ClientInfoCenter.txt" file (without a filename)

Return value:

0 = OK

1 = error

NcpClientCmd /ShowLogs

This function shows the stored log output in the console and writes the output to the Client log directory. If the parameter 1 is given, events will be logged until the process is interrupted with CTRL-C or the console is closed. The log output is stored for a maximum of the last seven days.

Command:

NcpClientCmd /showLogs [Timer]

Parameters:

Timer = number of seconds for recording the log output. If no value is given, only the current log output will be shown and saved.

Return value:

0 = OK

NcpClientCmd /firewallOff

The firewall can be disabled temporarily using this command. This function must be enabled in the firewall settings.

Command:

NcpClientCmd /firewallOff [Password]

Parameters:

Password = password that protects this function

Timeout = duration to disable firewall

Return value:

0 = OK - Firewall temporarily disabled

1 = error- incorrect parameter input

11 = error -firewall is not enabled

12 = error - authentication failed

13 = error - function is not permitted

14 = error - no timeout parameter entered

NcpClientCmd /firewallOn

This command reactivates the firewall before the duration specified when disabling the firewall temporarily.

Command:

NcpClientCmd /firewallOn

Parameters:

Return value:

0 = OK - firewall reactivated

11 = error- firewall is not activated

13 = error - function is not permitted

NcpClientCmd /actionUpdateOverLan

This command is called internally by the update client when the configuration is updated over the LAN. It starts the external applications configured in the client GUI under the "start external applications for configuration update via LAN" option.

The command line tool will check whether the GUI is started. If the GUI is started, the external applications are started. Otherwise the tool reads the configuration and starts the applications.

Command:

NcpClientCmd /actionUpdateOverLan

Parameters:

Return value:

0 = OK

NcpClientCmd /actionUpdateOverVpn

This command is called internally by the update client if the configuration is updated via VPN. It starts the external applications configured in the client GUI under the "start external applications for configuration update via VPN" option.

The command line tool will check whether the GUI is started. If the GUI is started, the external applications are started via the GUI, otherwise the tool will read the configuration and start the applications.

Command:

NcpClientCmd /actionUpdateOverVpn

Parameters:

Return value:

0 = OK

NcpClientCmd /CheckNewCert

This command is called internally by the update client if the configuration is updated. It checks whether a new certificate has been provided by the SEM.

Command:

NcpClientCmd /CheckNewCert

Parameters:

Return value:

0 = OK

NcpClientCmd /CheckNcpdb

This command is called internally by the update client if the license database (ncp.db) is changed.

Command:

NcpClientCmd /CheckNcpdb

Parameters:

Return value:

0 = OK

NcpClientCmd /ReadCnf

This command reads the configuration file (ncpphone.cfg) and SEM configuration if available (ncpphone.cng) and generates a new configuration file.

This command is called by the update client for a configuration update via LAN for reading and activating the configuration.

If the GUI is started, the new configuration will be read by the GUI, otherwise the configuration will be read by the command line tool.

Command:

NcpClientCmd /ReadCnf

Parameters:

Return value:

0 = OK

1 = failed

NcpClientCmd /getConnectionMedium

This command reads the actually used connection medium and returns the current connection medium via return code.

Command:

NcpClientCmd /getConnectionMedium

Parameters:

Return value:

- 1 = disconnection
  8 = LAN
18 = mobile network
20 = WLAN
21 = automatic media detection
100 = NCPRWSNT service not started

Advanced Functions with NCPRWSNT.EXE

The following advanced functions of the NCP client (with NCPRWSNT.EXE) can be used, provided the corresponding configuration parameters and their values are entered in the registry.

Parameter Values written by NCPRWSNT.EXE

```
64-bit: [HKEY_LOCAL_MACHINE\Software\\Wow6432Node\\NCP engineering GmbH\\NCP RWS/GA\\6.0]
```

```
32-bit: [HKEY_LOCAL_MACHINE\Software\\Ncp Engineering GmbH\\NCP RWS/GA\\6.0]
```

Key	Type	Meaning	Value
SecClCSI.	REG_DWORD	current connection state	1 = connected / 0 = disconnected
SecClFNDState	REG_DWORD	current fnd state	1 = fnd on an adapter / 0 = no fnd

Registry Parameters evaluated by NCPRWSNT.EXE

```
[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\ncprwsnt]
```

Key	Type	Meaning	Value
WlanUsed	String	Name of last used wifi adapter. Is used for re-enabling the adapter.	<some name>
SecCliDef	DWORD	enable firewall	0/1, default: 0
SecCliFw	DWORD	enable firewall	0/2, default: 0
FipsFallbackToNcpCrypto	DWORD	fallback to old crypto if FIPS failes to initialize	0/1, default: 0
DisableDPD	DWORD	no function in trunk r31002	0/1, default: 0
EnableDefGw	DWORD	set default gateway instead of half routes (see below)	0/1, default: 0
UseHighPrio	DWORD	set own process priority	0=NORMAL, 1=HIGH, default: 0
NoHideAdapter	DWORD		0=release ports, 1=don't release ports, default: 0
PreventIkePortRelease	DWORD	release ike sockets if not used	0/1, default: 0
Ikev2AuthFollowPrf	DWORD	special handling for IKEv2 "Digitale Signatur Algorithmus" (see below)	0/1, default: 0
FullTrace	DWORD	enable full trace. Don't forgot to turn it off when done!	0/1, 2=also enable driver trace, default: 0
FullTracePath	String	full filename of fulltrace log	default: "C:\ncptrace.log"

NoMbnConnection	DWORD	disable the use of MobileBroadband API	0/1, default: 0
PrgType	DWORD	disables some NAT	0/1, default: 0

Half Routes / Default Gateway

Using Half Routes instead of a default gateway for the virtual network adapter of the NCP client, there are problems with the NLA (Network Location Awareness) of Windows.

In the client code, the use of half routes is already activated via a "TRUE condition" by default. This is done by querying a corresponding registry key.

`[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\ncprwsnt]`

Key	Type	Value
EnableDefGw	REG_DWORD	0 - Half-Routes (Standardverhalten wie bisher) / 1 - Default Gateway

If this registry value does not exist, the client works like EnableDefGw = 0

IKEv2AuthFollowPRF

Valid from version 10.10.3

`[System\CurrentControlSet\Services\ncprwsnt]`

Key	Type	Value
Ikev2AuthFollowPrf	WORD	1

This is required if the "Digital Signature Algorithms" should follow the negotiated "PRF" instead of using the standard SHA1. In case of Cisco-ASA this will be done automatically without the need of this entry. This Entry will be obsolete as soon as all gateways follow the new RFC.

Routing Functionality of the Client

`[HKLM\System\CurrentControlSet\Services\ncprwsnt]`

Key	Type	Value	Description
SecClRtr.	REG_DWORD	0=disallow, 1=allow, default=0	Allow client to route
SecClRtrNet	REG_SZ	(example) 192.168.254.0/24,192.168.253.0/24	When routing allowed, specifies the source nets negotiated

Routing itself has to be enabled in the OS independently as its not done automatically.

`[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Tcpip\Parameters]`

Key	Type	Value
IPEnableRouter	REG_DWORD	1

DNS Handling on non NCP Adapters

Added support for a registry key for the control of DNS handling on non-NCP adapters when in connected state.

`[HKLM\System\CurrentControlSet\Services\ncprwsnt]`

Key	Type	Value
DNSHandling	DWORD (32-bit)	0=throw away /default), 1 = respond "no such name", 2 = icmp unreachable response, 3 = pass through

General registry values

ConnectState

The registry value returns the current connection status.

Registry Key

```
HKEY_LOCAL_MACHINE\SOFTWARE\NCP engineering GmbH\NCP Secure Client
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\NCP engineering GmbH\NCP Secure Client
```

Name

ConnectState

Parameter:

Values:

0 = Connection is disconnected

1 = Connection is established

2 = Connection is successfully established

3 = Internet connection is interrupted, VPN connection is held